# Contents

---

## About this guide
- Supported Fabric OS 6.x HP StorageWorks hardware .......................... 19
- Intended audience ........................................................................... 20
- Related documentation .................................................................. 20
- Document conventions and symbols .............................................. 20
- Rack stability .................................................................................. 21
- HP technical support .................................................................... 21
- Customer self repair ...................................................................... 21
- Product warranties ......................................................................... 21
- Subscription service ...................................................................... 22
  - HP websites ............................................................................... 22
- Documentation feedback ............................................................... 22

## 1 Standard features
- Overview ......................................................................................... 23
- Using the CLI .................................................................................. 23
- Connecting to the CLI ................................................................. 24
  - Using Telnet or SSH session ....................................................... 24
  - Using a console session on the serial port ................................. 25
- Changing passwords ...................................................................... 25
  - Changing default account passwords at login ............................ 26
- Configuring the Ethernet interface .............................................. 27
  - Displaying the network interface settings .................................. 27
  - Setting static Ethernet addresses ............................................. 28
  - Configuring DHCP ..................................................................... 29
  - Enabling DHCP ......................................................................... 29
  - Disabling DHCP ....................................................................... 29
- Setting the date and time .............................................................. 30
- Setting time zones ......................................................................... 30
- Synchronizing local time using NTP ............................................. 32
- Customizing switch names ............................................................ 33
- Working with Domain IDs ............................................................. 33
- Licensed features .......................................................................... 34
  - Generating a license key ............................................................ 35
  - Activating a license key .............................................................. 35
  - Removing a licensed feature ...................................................... 36
- Features and required licenses .................................................... 37
- Inter-Chassis Link (ICL) licensing ............................................... 38
- Time-based licenses ..................................................................... 39
  - High Availability considerations .............................................. 39
  - Firmware upgrade and downgrade consideration ...................... 39
    - Configupload and Configdownload considerations ................... 39
    - Expired licenses .................................................................... 39
- Ports on Demand (POD) licensing .............................................. 39
  - Activating POD ......................................................................... 40
  - Configuring Dynamic Ports on Demand .................................... 40
    - How ports are assigned to licenses ......................................... 40
    - Displaying the port license assignment ................................... 41
  - Activating Dynamic Ports on Demand ....................................... 41
  - Disabling Dynamic Ports on Demand ........................................ 42
  - Managing POD licenses ............................................................ 42
  - Reserving a license .................................................................... 42
  - Releasing a port ........................................................................ 43
  - Disabling and enabling switches ............................................... 44
Disabling and enabling ports ........................................... 44
Making basic connections ............................................. 45
   Connecting to devices ............................................ 45
   Connecting to other switches ................................. 45
Linking through a gateway ........................................... 45
Checking status ....................................................... 46
Tracking and controlling switch changes ....................... 48
Configuring the audit log ........................................... 50
   Auditable event classes ........................................ 51
Shutting down switches and Directors ......................... 53
High Availability of daemon processes ......................... 53

2 Managing user accounts ........................................... 55
Overview ........................................................................ 55
   Accessing the management channel ......................... 55
   Using Role-Based Access Control (RBAC) ................... 56
   Role permissions .................................................. 57
Managing the local database user accounts ..................... 59
   About the default accounts .................................... 59
   Defining local user accounts .................................. 59
   Recovering accounts ............................................. 62
   Changing local account passwords ......................... 62
Configuring the local user database .............................. 63
   Distributing the local user database ......................... 63
   Protecting the local user database from distributions .... 63
Configuring password policies ..................................... 64
   Setting the password strength policy ....................... 64
   Setting the password history policy ......................... 65
   Setting the password expiration policy ..................... 65
   Upgrade and downgrade considerations .................... 66
   Setting the account lockout policy ......................... 66
   Denial of service implications ............................... 67
Authentication model .................................................... 67
   Creating Fabric OS user accounts ......................... 69
   Managing Fabric OS users on the RADIUS server ........ 70
      Windows 2000 IAS ............................................. 70
      Linux FreeRadius server ..................................... 71
      RADIUS configuration and Admin Domains .............. 71
Configuring the RADIUS server ................................... 72
   Linux ............................................................... 72
   Windows 2000 ..................................................... 73
   LDAP configuration and Microsoft’s Active Directory .... 75
Configuring authentication servers on the switch ............. 77
Enabling and disabling local authentication as backup ....... 80
Boot PROM password ................................................... 80
   Setting the boot PROM password with a recovery string ... 81
      HP StorageWorks 4/8 or 4/16, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP 5530, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol (MP) Router ......................... 81
      4/256 SAN Director and DC SAN Backbone Director (short name, DC Director) .......... 82
   Setting the boot PROM password without a recovery string ... 83
      HP StorageWorks 4/8 or 4/16, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP 5530, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol (MP) Router ......................... 83
      4/256 SAN Director and DC SAN Backbone Director (short name, DC Director) .......... 83
Recovering forgotten passwords .................................. 84
3 Configuring standard security features ........................................... 85
   Secure protocols ............................................................... 85
   Ensuring network security .................................................. 86
   Configuring the Telnet protocol .......................................... 87
      Blocking Telnet ............................................................. 87
      Unblocking Telnet .......................................................... 87
   Blocking listeners ............................................................. 88
   Accessing switches and fabrics ........................................... 88
      Port configuration .......................................................... 89
   Configuring for the SSL protocol ........................................ 89
      Browser and Java support ................................................. 89
      Summary of SSL procedures ............................................. 90
      Choosing a CA ................................................................. 90
      Generating a public/private key ........................................... 90
      Generating and storing a CSR .......................................... 91
      Obtaining certificates ..................................................... 91
      Installing a switch certificate ......................................... 92
      Activating a switch certificate ........................................ 92
      Configuring the browser ................................................ 93
      Installing a root certificate to the Java plug-in ..................... 93
      Displaying and deleting certificates ................................ 94
      Troubleshooting certificates ........................................... 94
   Configuring for SNMP ....................................................... 95
      Setting the security level ................................................. 95
      Using the snmpConfig command ........................................ 96
   Configuring secure file copy ............................................... 98

4 Configuring advanced security features ................................... 99
   About access control list (ACL) policies ................................ 99
      How the ACL policies are stored ....................................... 99
      Identifying policy members ............................................. 100
   Configuring ACL policies ................................................ 100
      Displaying ACL policies ................................................ 101
      Configuring an FCS policy .............................................. 101
         FCS policy restrictions ............................................... 102
      Overview of steps to create and manage the FCS policies ....... 103
         Modifying the Primary FCS ............................................ 103
         Distributing an FCS policy ............................................ 104
      Configuring a DCC policy ................................................ 105
         DCC policy restrictions ................................................ 105
         Creating a DCC policy .................................................. 106
         Examples of creating DCC policies ................................ 107
      Creating an SCC policy ................................................... 107
   Saving changes to ACL policies ......................................... 108
   Activating changes to ACL policies .................................... 108
   Adding a member to an existing policy .................................. 108
   Removing a member from an ACL policy ................................ 109
   Deleting an ACL policy .................................................... 109
   Aborting all uncommitted changes ...................................... 109
   Configuring the authentication policy for fabric elements ....... 109
      E_Port authentication ..................................................... 110
      Device authentication policy .......................................... 112
      Auth policy restrictions ............................................... 112
         Supported configurations ............................................ 112
      Selecting authentication protocols .................................. 113
         Re-authenticating ports ............................................... 113
      Managing secret key pairs ............................................. 114
      Fabric wide distribution of the Auth policy ......................... 115
         Accept distributions configuration parameter .................. 116
# Maintaining configurations

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating an IP Filter policy</td>
<td>116</td>
</tr>
<tr>
<td>Cloning an IP Filter policy</td>
<td>116</td>
</tr>
<tr>
<td>Displaying an IP Filter policy</td>
<td>117</td>
</tr>
<tr>
<td>Saving an IP Filter policy</td>
<td>117</td>
</tr>
<tr>
<td>Activating an IP Filter policy</td>
<td>117</td>
</tr>
<tr>
<td>Deleting an IP Filter policy</td>
<td>118</td>
</tr>
<tr>
<td>IP Filter policy rules</td>
<td>118</td>
</tr>
<tr>
<td>IP Filter policy enforcement</td>
<td>119</td>
</tr>
<tr>
<td>Creating IP Filter policy rules</td>
<td>120</td>
</tr>
<tr>
<td>Deleting IP Filter policy rules</td>
<td>120</td>
</tr>
<tr>
<td>Aborting a switch session transaction</td>
<td>120</td>
</tr>
<tr>
<td>IP Filter policy distributions</td>
<td>121</td>
</tr>
<tr>
<td>IP Filter policy restrictions</td>
<td>121</td>
</tr>
<tr>
<td>Distributing the policy database</td>
<td>121</td>
</tr>
<tr>
<td>Configuring the database distribution settings</td>
<td>122</td>
</tr>
<tr>
<td>Distributing ACL policies to other switches</td>
<td>123</td>
</tr>
<tr>
<td>Setting the consistency policy fabric-wide</td>
<td>124</td>
</tr>
<tr>
<td>Notes on joining a switch to the fabric</td>
<td>125</td>
</tr>
<tr>
<td>Matching fabric-wide consistency policies</td>
<td>126</td>
</tr>
<tr>
<td>Non-matching fabric-wide consistency policies</td>
<td>127</td>
</tr>
<tr>
<td>FIPS support</td>
<td>127</td>
</tr>
<tr>
<td>Zeroization functions</td>
<td>128</td>
</tr>
<tr>
<td>Power-up self tests</td>
<td>128</td>
</tr>
<tr>
<td>Conditional tests</td>
<td>129</td>
</tr>
<tr>
<td>FIPS mode</td>
<td>130</td>
</tr>
<tr>
<td>Preparing the switch for FIPS</td>
<td>131</td>
</tr>
<tr>
<td>Overview of steps</td>
<td>131</td>
</tr>
</tbody>
</table>

## 5 Maintaining configurations

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintaining consistent configuration settings</td>
<td>135</td>
</tr>
<tr>
<td>Displaying configuration settings</td>
<td>135</td>
</tr>
<tr>
<td>Backing up a configuration</td>
<td>135</td>
</tr>
<tr>
<td>Troubleshooting configuration upload</td>
<td>136</td>
</tr>
<tr>
<td>Restoring switch information</td>
<td>137</td>
</tr>
<tr>
<td>Configuration download without disabling a switch</td>
<td>137</td>
</tr>
<tr>
<td>Security considerations</td>
<td>139</td>
</tr>
<tr>
<td>Troubleshooting configuration download</td>
<td>139</td>
</tr>
<tr>
<td>Messages captured in the logs</td>
<td>140</td>
</tr>
<tr>
<td>Restoring configurations in a FICON environment</td>
<td>140</td>
</tr>
<tr>
<td>Downloading configurations across a fabric</td>
<td>140</td>
</tr>
<tr>
<td>Configuration form</td>
<td>141</td>
</tr>
</tbody>
</table>

## 6 Managing administrative domains

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Domain features</td>
<td>143</td>
</tr>
<tr>
<td>Requirements for Admin Domains</td>
<td>145</td>
</tr>
<tr>
<td>User-defined Administrative Domains</td>
<td>145</td>
</tr>
<tr>
<td>System-defined Administrative Domains</td>
<td>145</td>
</tr>
<tr>
<td>AD0</td>
<td>146</td>
</tr>
<tr>
<td>AD255</td>
<td>146</td>
</tr>
<tr>
<td>Admin Domain access levels</td>
<td>147</td>
</tr>
<tr>
<td>Admin Domains and login</td>
<td>148</td>
</tr>
<tr>
<td>Admin Domain member types</td>
<td>148</td>
</tr>
<tr>
<td>Device members</td>
<td>148</td>
</tr>
<tr>
<td>Switch port members</td>
<td>149</td>
</tr>
<tr>
<td>Switch members</td>
<td>149</td>
</tr>
</tbody>
</table>
7 Installing and maintaining firmware .................................................. 165
About the firmware download process ................................................. 165
Upgrading and downgrading firmware ................................................ 166
Effects of firmware changes on accounts and passwords ....................... 166
Considerations for FICON CUP environments ..................................... 166
Preparing for firmware downloads ..................................................... 167
Checking connected switches ............................................................. 168
Obtaining and decompressing firmware .............................................. 169
Performing firmwareDownload on switches ......................................... 169
Overview of the firmware download process on switches ....................... 169
Downloading firmware to a Director ................................................. 170
Overview of the firmware download process on directors ....................... 172
4/256 SAN Director and DC Director firmwareDownload procedure ........ 172
Director restrictions for downgrading ............................................... 175
firmwareDownload from a USB device ............................................. 176
FIPS Support ......................................................................................... 177
Public and private key management ................................................... 177
The firmwareDownload command ...................................................... 178
Power-on firmware checksum test ...................................................... 179
Testing and restoring firmware on switches ....................................... 179
Testing and restoring firmware on directors ....................................... 180
Validating firmwareDownload ......................................................... 183
Troubleshooting firmwareDownload ................................................. 184
Considerations for downgrading firmware to Fabric OS 5.3.0 or earlier .... 184
Preinstallation messages ................................................................. 185
Blade troubleshooting tips ............................................................... 191
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining and naming zones</td>
<td>232</td>
</tr>
<tr>
<td>LSAN zones and fabric-to-fabric communications</td>
<td>232</td>
</tr>
<tr>
<td>LSAN zone binding (optional)</td>
<td>235</td>
</tr>
<tr>
<td>Dual backbone configuration</td>
<td>236</td>
</tr>
<tr>
<td>Maximum LSAN count</td>
<td>236</td>
</tr>
<tr>
<td>Configuring backbone fabrics for interconnectivity</td>
<td>237</td>
</tr>
<tr>
<td>HA and downgrade considerations</td>
<td>237</td>
</tr>
<tr>
<td>IPFC over FCR</td>
<td>237</td>
</tr>
<tr>
<td>Broadcast configuration</td>
<td>238</td>
</tr>
<tr>
<td>Monitoring resources</td>
<td>239</td>
</tr>
<tr>
<td>Routing ECHO</td>
<td>240</td>
</tr>
<tr>
<td>Upgrade and downgrade considerations</td>
<td>241</td>
</tr>
<tr>
<td>Interoperability with legacy FCR switches</td>
<td>241</td>
</tr>
<tr>
<td>Backward compatibility</td>
<td>242</td>
</tr>
<tr>
<td>Front domain consolidation</td>
<td>242</td>
</tr>
<tr>
<td>Using front domain consolidation</td>
<td>242</td>
</tr>
<tr>
<td>Range of output ports</td>
<td>243</td>
</tr>
<tr>
<td>Interoperating with an M-EOS fabric</td>
<td>245</td>
</tr>
<tr>
<td>McDATA Mi10K interoperability</td>
<td>246</td>
</tr>
<tr>
<td>Configuring the fabrics for interconnectivity</td>
<td>247</td>
</tr>
<tr>
<td>Connectivity modes</td>
<td>248</td>
</tr>
<tr>
<td>Configuring the FC router</td>
<td>248</td>
</tr>
<tr>
<td>Configuring M-EOS for interconnection</td>
<td>251</td>
</tr>
<tr>
<td>LSAN zoning with M-EOS</td>
<td>254</td>
</tr>
<tr>
<td>Completing the configuration</td>
<td>255</td>
</tr>
<tr>
<td>Migrating from an MP Router to a 400 MP Router</td>
<td>257</td>
</tr>
<tr>
<td>Configurations</td>
<td>257</td>
</tr>
<tr>
<td>Non-redundant configuration</td>
<td>257</td>
</tr>
<tr>
<td>Redundant configuration</td>
<td>258</td>
</tr>
<tr>
<td>Dual backbone configuration</td>
<td>258</td>
</tr>
<tr>
<td>Devices directly connected to router</td>
<td>259</td>
</tr>
<tr>
<td>11 Administering FICON fabrics</td>
<td>261</td>
</tr>
<tr>
<td>Overview of Fabric OS support for FICON</td>
<td>261</td>
</tr>
<tr>
<td>Supported switches</td>
<td>262</td>
</tr>
<tr>
<td>Types of FICON configurations</td>
<td>262</td>
</tr>
<tr>
<td>Control Unit Port (CUP)</td>
<td>262</td>
</tr>
<tr>
<td>FICON commands</td>
<td>263</td>
</tr>
<tr>
<td>User security considerations</td>
<td>264</td>
</tr>
<tr>
<td>Configuring switches</td>
<td>264</td>
</tr>
<tr>
<td>Preparing a switch</td>
<td>265</td>
</tr>
<tr>
<td>Configuring a single switch</td>
<td>265</td>
</tr>
<tr>
<td>Configuring a high-integrity fabric</td>
<td>265</td>
</tr>
<tr>
<td>Setting a unique Domain ID</td>
<td>266</td>
</tr>
<tr>
<td>Displaying information</td>
<td>267</td>
</tr>
<tr>
<td>Link incidents</td>
<td>267</td>
</tr>
<tr>
<td>Registered listeners</td>
<td>267</td>
</tr>
<tr>
<td>Node identification data</td>
<td>267</td>
</tr>
<tr>
<td>FRU failures</td>
<td>267</td>
</tr>
<tr>
<td>Swapping ports</td>
<td>268</td>
</tr>
<tr>
<td>Clearing the FICON management database</td>
<td>268</td>
</tr>
<tr>
<td>Using FICON CUP</td>
<td>268</td>
</tr>
<tr>
<td>Setup summary</td>
<td>269</td>
</tr>
<tr>
<td>Enabling and disabling FICON Management Server mode</td>
<td>269</td>
</tr>
<tr>
<td>Setting up CUP when FICON Management Server mode is enabled</td>
<td>270</td>
</tr>
<tr>
<td>Displaying the fmsmode setting</td>
<td>270</td>
</tr>
<tr>
<td>Displaying mode register bit settings</td>
<td>271</td>
</tr>
<tr>
<td>Setting mode register bits</td>
<td>272</td>
</tr>
<tr>
<td>Persistently enabling/disabling ports</td>
<td>272</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Configuring for syslogd.</td>
<td>296</td>
</tr>
<tr>
<td>Viewing equipment status</td>
<td>293</td>
</tr>
<tr>
<td>Viewing the system message log</td>
<td>294</td>
</tr>
<tr>
<td>Configuring for syslogd.</td>
<td>296</td>
</tr>
<tr>
<td>Viewing the port log</td>
<td>294</td>
</tr>
<tr>
<td>Configuring the host.</td>
<td>296</td>
</tr>
<tr>
<td>Configuring the switch</td>
<td>297</td>
</tr>
<tr>
<td>Viewing and saving diagnostic information</td>
<td>298</td>
</tr>
<tr>
<td>Setting up automatic trace dump transfers</td>
<td>298</td>
</tr>
<tr>
<td>Troubleshooting questions</td>
<td>302</td>
</tr>
<tr>
<td>Port and switch naming standards</td>
<td>273</td>
</tr>
<tr>
<td>Adding and removing FICON CUP licenses</td>
<td>273</td>
</tr>
<tr>
<td>Zoning and PDCM considerations</td>
<td>273</td>
</tr>
<tr>
<td>Zoning and link incident reporting</td>
<td>273</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>274</td>
</tr>
<tr>
<td>Identifying ports</td>
<td>274</td>
</tr>
<tr>
<td>Backing up and restoring FICON configuration files</td>
<td>275</td>
</tr>
<tr>
<td>Recording configuration information</td>
<td>276</td>
</tr>
<tr>
<td>Sample IOCP configuration file</td>
<td>277</td>
</tr>
<tr>
<td>12 Configuring the Distributed Management Server</td>
<td>279</td>
</tr>
<tr>
<td>Introduction</td>
<td>279</td>
</tr>
<tr>
<td>Enabling and disabling the platform services</td>
<td>279</td>
</tr>
<tr>
<td>Controlling access</td>
<td>280</td>
</tr>
<tr>
<td>Configuring the server database</td>
<td>283</td>
</tr>
<tr>
<td>Controlling topology discovery</td>
<td>283</td>
</tr>
<tr>
<td>13 Working with Diagnostic Features</td>
<td>285</td>
</tr>
<tr>
<td>About Fabric OS diagnostics</td>
<td>285</td>
</tr>
<tr>
<td>Viewing power-on self test</td>
<td>285</td>
</tr>
<tr>
<td>Viewing switch status</td>
<td>287</td>
</tr>
<tr>
<td>Viewing port information</td>
<td>289</td>
</tr>
<tr>
<td>Viewing the system message log</td>
<td>294</td>
</tr>
<tr>
<td>Allergy and saving diagnostic information</td>
<td>298</td>
</tr>
<tr>
<td>Setting up automatic trace dump transfers</td>
<td>298</td>
</tr>
<tr>
<td>14 Troubleshooting</td>
<td>301</td>
</tr>
<tr>
<td>About troubleshooting</td>
<td>301</td>
</tr>
<tr>
<td>Most common problem areas</td>
<td>301</td>
</tr>
<tr>
<td>Gathering information for technical support</td>
<td>302</td>
</tr>
<tr>
<td>Troubleshooting questions</td>
<td>302</td>
</tr>
<tr>
<td>Analyzing connection problems</td>
<td>304</td>
</tr>
<tr>
<td>Restoring a segmented fabric</td>
<td>307</td>
</tr>
<tr>
<td>Correcting zoning setup issues</td>
<td>309</td>
</tr>
<tr>
<td>Recognizing MQ-WRITE errors</td>
<td>311</td>
</tr>
<tr>
<td>Correcting I2C bus errors</td>
<td>312</td>
</tr>
<tr>
<td>Correcting device login issues</td>
<td>313</td>
</tr>
<tr>
<td>Identifying media-related issues</td>
<td>315</td>
</tr>
<tr>
<td>Correcting link failures</td>
<td>317</td>
</tr>
<tr>
<td>Correcting marginal links</td>
<td>319</td>
</tr>
<tr>
<td>Inaccurate information in the system message log</td>
<td>320</td>
</tr>
<tr>
<td>Tracing Fibre Channel information</td>
<td>320</td>
</tr>
<tr>
<td>Configuring ftrace for a tunnel</td>
<td>321</td>
</tr>
<tr>
<td>Displaying ftrace for a tunnel</td>
<td>321</td>
</tr>
<tr>
<td>Recognizing port initialization and FCP auto discovery process</td>
<td>322</td>
</tr>
<tr>
<td>Using port mirroring</td>
<td>322</td>
</tr>
<tr>
<td>Supported hardware</td>
<td>323</td>
</tr>
<tr>
<td>Port mirroring considerations</td>
<td>324</td>
</tr>
<tr>
<td>Creating, deleting, and displaying port mirroring</td>
<td>324</td>
</tr>
</tbody>
</table>
15 Administering NPIV ................................................................. 327
   About NPIV ........................................................................ 327
   Enabling and disabling NPIV .............................................. 327
   Configuring NPIV ................................................................ 327
      Configuration scenarios .................................................. 328
   Viewing NPIV port configuration information ..................... 328
   Displaying login information ............................................ 330

16 Optimizing fabric behavior .................................................. 331
   Introduction to adaptive networking .................................... 331
   Top Talkers ....................................................................... 331
   Traffic Isolation .................................................................. 331
      Ti zone failover ............................................................... 332
      FSPF routing rules and Traffic Isolation ......................... 332
      General rules for Ti zones .............................................. 333
         Supported configurations for Traffic Isolation ............... 334
         Limitations and restrictions of Traffic Isolation ............ 335
         Admin Domain considerations for Traffic Isolation ....... 335
      Creating a Ti zone .......................................................... 335
      Modifying Ti zones ........................................................ 336
      Activating and deactivating a Ti zone ............................. 337
      Deleting a Ti zone .......................................................... 338
      Displaying Ti zones ....................................................... 338
   QoS: ingress rate limiting .................................................. 338
   QoS: SID/DID traffic prioritization ..................................... 339
   QoS zones ....................................................................... 340
   QoS on E Ports .................................................................. 341
   Supported configurations for traffic prioritization ............... 341
   Setting traffic prioritization ............................................. 342

17 Administering Advanced Performance Monitoring .................. 343
   About Advanced Performance Monitoring ....................... 343
   Monitoring AL_PAs .......................................................... 345
   Monitoring end-to-end performance ................................... 345
      Adding end-to-end monitors ........................................... 346
      Setting a mask for end-to-end monitors ......................... 347
      Deleting end-to-end monitors ....................................... 348
   Monitoring filter-based performance ................................. 349
      Adding standard filter-based monitors ......................... 349
      Adding custom filter-based monitors ............................ 350
      Deleting filter-based monitors .................................... 351
   Monitoring ISL performance ............................................. 351
   Identifying top bandwidth users (Top Talkers) .................... 352
      Using Top Talker monitors in port mode ....................... 353
      Using Top Talker monitors in fabric mode ..................... 354
      Limitations of Top Talker monitors ............................... 355
   Monitoring trunks .............................................................. 355
   Displaying monitor counters ............................................. 355
      Known display problem and workaround ....................... 359
   Clearing monitor counters ............................................... 359
   Saving and restoring monitor configurations .................... 361
   Collecting performance data ............................................ 361

18 Administering Extended Fabrics .......................................... 363
   Extended Fabrics licensing ................................................ 363
   Extended Fibre Channel over distance ............................... 363
      Distance levels for extended Inter-Switch Links (ISLs) .... 363
      Buffer-to-Buffer Credits .............................................. 363
      FC switch port Buffer Credit requirements for long distance calculations ........................................ 365
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual port types</td>
<td>417</td>
</tr>
<tr>
<td>Compression</td>
<td>418</td>
</tr>
<tr>
<td>Traffic shaping</td>
<td>418</td>
</tr>
<tr>
<td>QoS concepts and implementation over FCIP</td>
<td>418</td>
</tr>
<tr>
<td>Layer three DiffServ Code Points (DSCP)</td>
<td>419</td>
</tr>
<tr>
<td>VLAN tagging and layer two class of service (L2CoS)</td>
<td>419</td>
</tr>
<tr>
<td>When both DSCP and L2CoS are used.</td>
<td>419</td>
</tr>
<tr>
<td>IPSec concepts and implementation over FCIP</td>
<td>420</td>
</tr>
<tr>
<td>Options for enhancing tape write I/O performance</td>
<td>421</td>
</tr>
<tr>
<td>FCIP fastwrite and tape pipelining</td>
<td>421</td>
</tr>
<tr>
<td>Constraints for FCIP fastwrite and tape pipelining</td>
<td>422</td>
</tr>
<tr>
<td>FCIP fastwrite/tape pipelining configurations</td>
<td>422</td>
</tr>
<tr>
<td>Unsupported configurations</td>
<td>423</td>
</tr>
<tr>
<td>FICON emulation concepts</td>
<td>424</td>
</tr>
<tr>
<td>XRC emulation</td>
<td>425</td>
</tr>
<tr>
<td>Tape write pipelining</td>
<td>425</td>
</tr>
<tr>
<td>Tape read pipelining</td>
<td>425</td>
</tr>
<tr>
<td>Device level acknowledgment</td>
<td>425</td>
</tr>
<tr>
<td>TIN/TIR emulation</td>
<td>425</td>
</tr>
<tr>
<td>Read block ID emulation</td>
<td>425</td>
</tr>
<tr>
<td>FTRACE concepts</td>
<td>425</td>
</tr>
<tr>
<td>FCIP services configuration guidelines</td>
<td>426</td>
</tr>
<tr>
<td>Checklist for configuring FCIP links</td>
<td>426</td>
</tr>
<tr>
<td>Configuring IPSec</td>
<td>427</td>
</tr>
<tr>
<td>IPSec parameters</td>
<td>428</td>
</tr>
<tr>
<td>Managing policies</td>
<td>429</td>
</tr>
<tr>
<td>Persistently disabling ports</td>
<td>431</td>
</tr>
<tr>
<td>Configuring VEX ports</td>
<td>431</td>
</tr>
<tr>
<td>Configuring IP interfaces and IP routes</td>
<td>432</td>
</tr>
<tr>
<td>Configuring FCIP tunnels</td>
<td>434</td>
</tr>
<tr>
<td>Configuring FICON emulation</td>
<td>435</td>
</tr>
<tr>
<td>Configuring FTRACE</td>
<td>437</td>
</tr>
<tr>
<td>Verifying the FCIP tunnel configuration</td>
<td>437</td>
</tr>
<tr>
<td>Enabling persistently disabled ports</td>
<td>440</td>
</tr>
<tr>
<td>Modify and delete command options</td>
<td>442</td>
</tr>
<tr>
<td>Modifying FCIP tunnels</td>
<td>442</td>
</tr>
<tr>
<td>Modifying/deleting QoS Settings</td>
<td>443</td>
</tr>
<tr>
<td>FICON emulation modify operations</td>
<td>443</td>
</tr>
<tr>
<td>Deleting an fcip tunnel</td>
<td>445</td>
</tr>
<tr>
<td>Deleting an IP interface (IPIF)</td>
<td>445</td>
</tr>
<tr>
<td>Deleting an IRoute</td>
<td>445</td>
</tr>
<tr>
<td>Deleting an FTRACE configuration</td>
<td>445</td>
</tr>
<tr>
<td>Maintaining VLAN tag tables</td>
<td>445</td>
</tr>
<tr>
<td>Troubleshooting FCIP links</td>
<td>446</td>
</tr>
<tr>
<td>WAN performance analysis tools</td>
<td>447</td>
</tr>
<tr>
<td>About the iperf option</td>
<td>447</td>
</tr>
<tr>
<td>Running WAN tool sessions with an FCIP tunnel online</td>
<td>447</td>
</tr>
<tr>
<td>FCIP port bandwidth</td>
<td>447</td>
</tr>
<tr>
<td>WAN tool performance characteristics</td>
<td>448</td>
</tr>
<tr>
<td>Starting WAN tool analysis</td>
<td>448</td>
</tr>
<tr>
<td>WAN tool ipPerf syntax</td>
<td>449</td>
</tr>
<tr>
<td>Using portCmd ping</td>
<td>450</td>
</tr>
<tr>
<td>Using portCmd traceroute</td>
<td>451</td>
</tr>
<tr>
<td>FCIP tunnel performance characteristics</td>
<td>452</td>
</tr>
<tr>
<td>FICON performance statistics</td>
<td>455</td>
</tr>
<tr>
<td>FTRACE output control and display</td>
<td>456</td>
</tr>
<tr>
<td>FC fastwrite concepts</td>
<td>457</td>
</tr>
<tr>
<td>Platforms and OS requirements for FC fastwrite</td>
<td>458</td>
</tr>
<tr>
<td>Constraints for FC fastwrite</td>
<td>458</td>
</tr>
</tbody>
</table>
How FC fastwrite works ......................................................... 458
FC fastwrite flow configuration requirements .......................... 459
Hardware considerations for FC fastwrite ............................... 459
Configuring and enabling FC fastwrite ................................. 460
Disabling FC fastwrite on a blade or switch ......................... 462
Disabling FC fastwrite on a port ......................................... 462

A Configuring the PID format .............................................. 463
About PIDs and PID binding ................................................. 463
Summary of PID formats ...................................................... 463
Impact of changing the fabric PID format ............................... 464
Host reboots ........................................................................ 464
Static PID mapping errors .................................................... 464
Changes to configuration data .............................................. 465
Selecting a PID format ......................................................... 465
Evaluating the fabric .......................................................... 466
Planning the update procedure ............................................ 468
Online update ....................................................................... 468
Offline update ....................................................................... 469
Hybrid update ...................................................................... 469
Changing to core PID format ............................................... 469
Converting port number to area ID ....................................... 470
Performing PID format changes ........................................... 472
Basic procedure .................................................................... 472
HP/UX procedure .................................................................. 473
AIX procedure ...................................................................... 475
Swapping port area IDs ....................................................... 476

B Implementing an interoperable fabric .................................. 477
Overview ............................................................................ 477
Understanding Brocade and McDATA interoperability ............ 477
Determining McDATA-aware features ................................... 477
Determining McDATA-unaware features ............................... 478
Supported Connectivity for Fabric 6.0 ................................. 479
Feature support and interoperability ...................................... 479
M-EOS 9.6.2 features supported in Fabric OS 6.0 .................. 481
Port number offset ............................................................... 481
NPIV .................................................................................. 481
Trunking ............................................................................. 482
M-EOS 9.6.2 features not supported by Fabric OS 6.0 .......... 482
Domain ID offset configuration ............................................ 482
Diagnostic test differences .................................................. 482
Optional 6.0 licensing ......................................................... 482
Supported switches ............................................................. 483
Supported features McDATA Fabric mode (interopmode 2) .. 484
Supported features McDATA Open Fabric mode (interopmode 3) ................................................................. 484
Unsupported features McDATA Fabric and Open Fabric modes ................................................................. 484
McDATA Fabric mode configuration restrictions .................. 484
McDATA Open Fabric mode configuration restrictions ........ 485
Upgrade and downgrade restrictions .................................... 485
Zoning restrictions ............................................................. 485
Zone name restrictions ....................................................... 486
Activating zones in McDATA Fabric mode ........................... 486
Default zone ....................................................................... 486
Safe zone ............................................................................ 487
Activating zone configurations on a standalone switch ....... 487
Activating zone configurations fabric-wide ......................... 487
Verifying the effective zone configuration ........................... 487
Moving to McDATA Open Fabric mode from earlier Fabric OS versions ................................................................. 489
About this guide

This guide provides information about:

- Installing and configuring Fabric OS 6.x
- Managing user accounts
- Using licensed features

Supported Fabric OS 6.x HP StorageWorks hardware

Table 1 lists Brocade and HP StorageWorks product models supported by Fabric OS 6.x.

<table>
<thead>
<tr>
<th>Brocade product name</th>
<th>Equivalent HP StorageWorks B-Series product name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade 200E switch</td>
<td>HP StorageWorks 4/8 SAN Switch or HP StorageWorks 4/16 SAN Switch</td>
</tr>
<tr>
<td>Brocade 3250 switch switch</td>
<td>HP StorageWorks SAN Switch 2/8V</td>
</tr>
<tr>
<td>Brocade 3850 switch</td>
<td>HP StorageWorks SAN Switch 2/16V</td>
</tr>
<tr>
<td>Brocade 3900 switch</td>
<td>HP StorageWorks SAN Switch 2/32</td>
</tr>
<tr>
<td>Brocade 4100 switch</td>
<td>HP StorageWorks SAN Switch 4/32</td>
</tr>
<tr>
<td>Brocade 4900 switch</td>
<td>HP StorageWorks 4/64 SAN Switch</td>
</tr>
<tr>
<td>Brocade 24000 Director</td>
<td>HP StorageWorks SAN Director 2/128</td>
</tr>
<tr>
<td>Brocade 48000 Director</td>
<td>HP StorageWorks 4/256 SAN Director</td>
</tr>
<tr>
<td>Brocade FC4-16 Blade</td>
<td>HP StorageWorks 16 Port 4Gb Blade</td>
</tr>
<tr>
<td>Brocade FC4-32 Blade</td>
<td>HP StorageWorks 32 Port 4Gb Blade</td>
</tr>
<tr>
<td>FR4-18i blade</td>
<td>B-Series Multi-protocol (MP) Router blade</td>
</tr>
<tr>
<td>FC4-48 Blade</td>
<td>HP StorageWorks 4/48 SAN Director Blade</td>
</tr>
<tr>
<td>FC4-16IP Blade</td>
<td>HP StorageWorks iSCSI Director Blade (compatible with HP StorageWorks 4/256 SAN Director only)</td>
</tr>
<tr>
<td>Brocade 7500</td>
<td>HP StorageWorks 400 Multi-protocol (MP) Router</td>
</tr>
<tr>
<td>Brocade 4012</td>
<td>Brocade 4Gb SAN Switch for HP p-Class BladeSystem</td>
</tr>
<tr>
<td>Brocade 4024</td>
<td>Brocade 4Gb SAN Switch for HP c-Class BladeSystem</td>
</tr>
<tr>
<td>Brocade 5000</td>
<td>HP StorageWorks SAN Switch 4/32</td>
</tr>
<tr>
<td>Brocade DCX Backbone</td>
<td>HP StorageWorks DC SAN Backbone Director (short name, DC Director)</td>
</tr>
<tr>
<td>FC10-6 Blade</td>
<td>HP StorageWorks SAN Director 6 Port 10Gb FC blade</td>
</tr>
<tr>
<td>FC8-16 Blade</td>
<td>HP StorageWorks SAN Director 16 Port 8Gb FC blade</td>
</tr>
<tr>
<td>FC8-32 Blade</td>
<td>HP StorageWorks SAN Director 32 Port 8Gb FC blade</td>
</tr>
<tr>
<td>FC8-48 Blade</td>
<td>HP StorageWorks SAN Director 48 Port 8Gb FC blade</td>
</tr>
</tbody>
</table>
Intended audience

This guide is intended for system administrators with knowledge of:

- Storage area networks
- HP StorageWorks Fibre Channel SAN switches

Related documentation

The following documents provide related information:

- HP StorageWorks Fabric OS 6.x release notes
- HP StorageWorks DC SAN Backbone Director hardware reference guide

You can find these documents from the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

In the Storage section, click Storage Networking and then select your product.

Document conventions and symbols

Table 2 Document conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue text: Table 1</td>
<td>Cross-reference links and e-mail addresses</td>
</tr>
<tr>
<td>Blue, underlined text: <a href="http://www.hp.com">http://www.hp.com</a></td>
<td>Website addresses</td>
</tr>
<tr>
<td><strong>Bold text</strong></td>
<td>• Key that are pressed</td>
</tr>
<tr>
<td></td>
<td>• Text typed into a GUI element, such as into a box</td>
</tr>
<tr>
<td></td>
<td>• GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes</td>
</tr>
<tr>
<td><em>Italics text</em></td>
<td>Text emphasis</td>
</tr>
<tr>
<td><strong>Monospace text</strong></td>
<td>• File and directory names</td>
</tr>
<tr>
<td></td>
<td>• System output</td>
</tr>
<tr>
<td></td>
<td>• Code</td>
</tr>
<tr>
<td></td>
<td>• Commands, their arguments, and argument values</td>
</tr>
<tr>
<td><strong>Monospace, italic text</strong></td>
<td>• Code variables</td>
</tr>
<tr>
<td></td>
<td>• Command variables</td>
</tr>
<tr>
<td><strong>Monospace, bold text</strong></td>
<td>Emphasized monospace text</td>
</tr>
</tbody>
</table>

⚠️ **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

⚠️ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

💾 **IMPORTANT:** Provides clarifying information or specific instructions.
NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

Rack stability

Rack stability protects personnel and equipment.

WARNING!

To reduce the risk of personal injury or damage to equipment:

• Extend leveling jacks to the floor.
• Ensure that the full weight of the rack rests on the leveling jacks.
• Install stabilizing feet on the rack.
• In multiple-rack installations, secure racks together.
• Extend only one rack component at a time. Racks may become unstable if more than one component is extended.

HP technical support

For worldwide technical support information, see the HP support website:

http://www.hp.com/support/

Before contacting HP, collect the following information:

• Product model names and numbers
• Technical support registration number (if applicable)
• Product serial numbers
• Error messages
• Operating system type and revision level
• Detailed questions

Customer self repair

HP customer self repair (CSR) programs allow you to repair your StorageWorks product. If a CSR part needs replacing, HP ships the part directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your HP-authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider. For North America, see the CSR website:

http://www.hp.com/go/selfrepair

Product warranties

For information about HP StorageWorks product warranties, see the warranty information website:

http://www.hp.com/go/storagewarranty
Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website: http://www.hp.com/go/e-updates.

After registering, you will receive e-mail notification of product enhancements, new driver versions, firmware updates, and other product resources.

HP websites

For additional product information, see the following HP websites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/manuals

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to storagedocs.feedback@hp.com. All submissions become the property of HP.
1 Standard features

This chapter describes how to configure your HP StorageWorks SAN using the Fabric OS Command Line Interface (CLI). Before you can configure a Storage Area Network (SAN), you must power-up the Director or switch and blades, and then set the IP addresses of those devices. Although this chapter focuses on configuring a SAN using the CLI, you can also use the following methods to configure a SAN:

- Web Tools
  For Web Tools procedures, see the Web Tools Administrator's Guide.
- Fabric Manager
  For Fabric Manager procedures, see the Fabric Manager Administrator’s Guide.

Overview

As a result of the differences between fixed-port and variable-port devices, procedures sometimes differ among HP switch models. As new models are introduced, new features sometimes apply only to specific switches.

When procedures or parts of procedures apply to some models but not others, this guide identifies the specifics for each model. For example, a number of procedures that apply only to variable-port devices are found in “Configuring Directors” on page 193.

Although many different software and hardware configurations are tested and supported, documenting all possible configurations and scenarios is beyond the scope of this document. In some cases, earlier releases are highlighted to present considerations for interoperating with them.

The hardware reference manuals for HP products describe how to power up devices and set their IP addresses. After the IP address is set, you can use the CLI procedures contained in this guide.

For additional information about the commands used in the procedures, see online help or the Fabric OS Command Reference.

Using the CLI

Fabric OS 6.x uses Role-Based Access Control (RBAC) to control access to all Fabric OS operations. You can display a list of all command help topics for a given login level. For example, if you are logged in as user and enter the `help` command, a list of all user-level commands that can be executed is displayed. The same rule applies to the admin, securityAdmin, and the switchAdmin roles.

**NOTE:** When command examples in this guide show user input enclosed in quotation marks, the quotation marks are required.

You can enter the `help [ | more ]` (pipe more) command with no specific command and all commands display. The `| more` argument displays the command one page at a time. Or, you can enter `help <command>`, where command is the name of the command for which you need specific information.
The following commands provide help files for specific topics to understand configuring your SAN:

- diagHelp: Diagnostic help information
- ficonHelp: FICON help information
- fwHelp: Fabric Watch help information
- iscsiHelp: iSCSI help information
- licenseHelp: License help information
- perfHelp: Performance Monitoring help information
- routeHelp: Routing help information
- trackChangesHelp: Track Changes help information
- zoneHelp: Zoning help information

---

**Connecting to the CLI**

Read this section for procedures.

**Using Telnet or SSH session**

Connect to the Fabric OS through a Telnet or SSH connection or through a console session on the serial port. The switch must also be physically connected to the network. If the switch network interface is not configured or the switch has been disconnected from the network, use a console session on the serial port as described in the next section.

**NOTE:** To automatically configure the network interface on a DHCP-enabled switch, plug the switch into the network and power it on. The DHCP client automatically gets the IP and gateway addresses from the DHCP server. The DHCP server must be on the same subnet as the switch. See “Configuring DHCP” on page 29 for more details.

**Rules for Telnet connections:**

- Never change the IP address of the switch while two Telnet sessions are active; if you do, your next attempt to log in fails. To recover, gain access to the switch by one of these methods:
  - You can use Web Tools to perform a fast boot. When the switch comes up, the Telnet quota is cleared. (For instructions on performing a fast boot with Web Tools, see the Web Tools Administrator’s Guide.)
  - If you have the required privileges, you can connect through the serial port, log in as root, and use operating system commands to identify and kill the Telnet processes without disrupting the fabric.
- For admin level accounts, Fabric OS limits the number of simultaneous Telnet sessions per switch to two. For more details on session limits, see “Configuring the Telnet protocol” on page 87 and “Managing user accounts” on page 55.

**To connect using Telnet:**

1. Verify that the switch’s network interface is configured and that it is connected to the IP network through the RJ-45 Ethernet port.
   Switches in the fabric that are not connected through the Ethernet can be managed through switches that are using IP over Fibre Channel. The embedded port must have an assigned IP address.

2. Open a Telnet connection using the IP address of the logical switch to which you want to connect.
   Enter the account ID at the login prompt.
   See “Changing passwords” on page 25 for instructions on how to log in for the first time.

3. Enter the password.
   If you have not changed the system passwords from the default, you are prompted to change them.
   Enter the new system passwords, or press Ctrl-C to skip the password prompts. See “Changing default account passwords at login” on page 26.
4. Verify that the login was successful.
   The prompt displays the switch name and user ID to which you are connected.
   
   login: admin
   password: xxxxxxx
   switch:admin>

Using a console session on the serial port

Note the following behaviors for serial connections:

- Some procedures require that you connect through the serial port; for example, setting the IP address or
  setting the boot PROM password.
- If you are using a Fabric OS version prior to 6.x, and secure mode is enabled, connect through the
  serial port of the primary FCS switch.
- **4/256 SAN Director and DC Director:** You can connect to CP0 or CP1 using either of the two
  serial ports.

To connect through the serial port:

1. Connect the serial cable to the serial port on the switch and to an RS-232 serial port on the workstation.
   If the serial port on the workstation is RJ-45 instead of RS-232, remove the adapter on the end of the
   serial cable and insert the exposed RJ-45 connector into the RJ-45 serial port on the workstation.

2. Open a terminal emulator application (such as HyperTerminal on a PC, or TERM, TIP, or Kermit in a
   UNIX environment), and configure the application as follows:
   - In a Windows environment:
     
     Parameter | Value  
     ----------|--------
     Bits per second | 9600  
     Databits | 8  
     Parity | None  
     Stop bits | 1  
     Flow control | None  

   - In a UNIX environment, enter the following string at the prompt:
     
     tip /dev/ttyb -9600

     If ttyb is already in use, use ttya instead and enter the following string at the prompt:
     
     tip /dev/ttya -9600

Changing passwords

The switch automatically prompts you to change the default account passwords after logging in for the first

   time. If you do not change the passwords, the switch prompts you after each subsequent login until all the
   default passwords have been changed.

**NOTE:** The default account passwords can be changed from their original value only when prompted

   immediately following the login; the passwords cannot be changed using the passwd command later in
   the session. If you skip the prompt, and then later decide to change the passwords, log out and then back
   in.

The default accounts on the switch are admin, user, root, and factory. Use the default administrative

   account as shown in Table 3 to log into the switch for the first time and to perform the basic configuration
   tasks.
Every logical switch (domain) has a set of default accounts. The root and factory default accounts are reserved for development and manufacturing. The user account is primarily used for system monitoring. For more information on default accounts, see “About the default accounts” on page 59.

Table 3 describes the default administrative accounts for switches by model number.

### Table 3  Default administrative account names and passwords

<table>
<thead>
<tr>
<th>Model</th>
<th>Administrative account</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/256 SAN Director and DC SAN Backbone Director (short name, DC Director)</td>
<td>admin</td>
<td>password</td>
</tr>
</tbody>
</table>

### Changing default account passwords at login

The change default account passwords prompt accepts a maximum of eight characters. Any characters beyond the eighth character are ignored. Only the default password is subject to the eight character limit. User-defined passwords can have 8 to 40 characters. They must begin with an alphabetic character and can include numeric characters, the period (.), and the underscore (_). They are case-sensitive, and they are not displayed when you enter them on the command line.

Record the passwords exactly as entered and store them in a secure place because recovering passwords requires significant effort and fabric downtime. Although the root and factory accounts are not meant for general use, change their passwords if prompted to do so and save the passwords in case they are needed for recovery purposes.

To change the default account passwords at login:

1. Connect to the switch and log in using the default administrative account.
2. At each of the “Enter new password” prompts, either enter a new password or skip the prompt.

To skip a single prompt press Enter. To skip all of the remaining prompts press Ctrl-c.

```
login: admin
Password:
Please change your passwords now.
Use Control-C to exit or press 'Enter' key to proceed.
for user - root
Changing password for root
Enter new password: ********
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.
Please change your passwords now.
for user - factory
Changing password for factory
Enter new password: ********
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.
Please change your passwords now.
for user - admin
Changing password for admin
Enter new password: ********
Password changed.
Saving password to stable storage.
Password saved to stable storage successfully.
Please change your passwords now.
for user - user
Changing password for user
Enter new password: ********
```
Configuring the Ethernet interface

You can use Dynamic Host Configuration Protocol (DHCP) for the Ethernet network interface configuration. The Ethernet (network) interface provides management access, including direct access to the Fabric OS CLI, and allows other tools, such as Web Tools, to interact with the switch.

You can continue to use a static Ethernet addressing system or allow the DHCP client to automatically acquire Ethernet addresses. Configure the Ethernet interface IP, subnet mask, and gateway addresses in one of the following manners:

- “Setting static Ethernet addresses” on page 28
- “Configuring DHCP” on page 29

When you change the Ethernet interface settings, open connections such as SSH or Telnet may be dropped. Reconnect using the new Ethernet IP information or change the Ethernet settings using a console session through the serial port to maintain your session through the change. You must connect through the serial port to set the Ethernet IP address if the Ethernet network interface is not configured already.

Displaying the network interface settings

If an IP address has not been assigned to the network interface (Ethernet), you must connect to the Fabric OS CLI using a console session on the serial port. For more information, see “Using a console session on the serial port” on page 25. Otherwise, connect using SSH.

To display the network interface settings:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `ipAddrShow` command.

```
switch:admin> ipAddrShow
```

```
switch:admin> ipAddrShow
Ethernet IP Address: 102.108.153.238
Ethernet Subnetmask: 255.255.255.0
Fibre Channel IP Address: none
Fibre Channel Subnetmask: 255.255.0.0
Gateway IP Address: 102.108.153.1
DHCP: Off
IPv6 Autoconfiguration Enabled: No
Local IPv6 Addresses: static 1080::9:800:400c:416a/64
```

If the Ethernet IP address, subnet mask, and gateway address are displayed, then the network interface is configured. Verify that the information is correct. If DHCP is enabled, the network interface information was acquired from the DHCP server.

**NOTE:** You can use either IPv4 or IPv6 with a classless inter-domain routing (CIDR) block notation to set up your IP addresses.
Setting static Ethernet addresses

Use static Ethernet network interface addresses on HP StorageWorks 2/128, 4/256 SAN Director, DC Director models, and in environments where DHCP service is not available. To use static addresses for the Ethernet interface, you must first disable DHCP. You may enter static Ethernet information and disable DHCP at the same time. Refer to “Configuring DHCP” on page 29 for more information.

If you choose not to use DHCP or to specify an IP address for your switch Ethernet interface, you can do so by entering none or 0.0.0.0 in the Ethernet IP address field.

**IMPORTANT:** IP address 0.0.0.0 is not supported in Fabric OS versions earlier than 5.2.0.

To set static addresses for the Ethernet network interface:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the following command to set the IPv4 address:

   switch:admin> ipaddrset
   Ethernet IP Address [192.168.74.102]:
   Ethernet Subnetmask [255.255.255.0]:
   Fibre Channel IP Address [220.220.220.2]:
   Fibre Channel Subnetmask [255.255.0.0]:
   Gateway IP Address [192.168.74.1]:
   DHCP [OFF]: off

   or to set an IPv6 address on a switch:

   switch:admin> ipaddrset -ipv6 --add 1080::8:800:200C:417A/64
   IP address is being changed...Done.

   Example of setting logical switch (sw0)'s IPv6 address on a Director:

   director:admin> ipaddrset -ipv6 -sw 0 --add 1080::8:800:200C:417B/64
   IP address is being changed...Done.

   Enter the network information in dotted decimal notation for the Ethernet IPv4 address and in semicolon separated notation for IPv6. Enter the Ethernet Subnetmask and Gateway Address at the prompts. Skip Fibre Channel prompts by pressing Enter. Disable DHCP by entering OFF.

   On an AP blade, configure the two external Ethernet interfaces to two different subnets, or if two subnets are not present, configure one of the interfaces and leave the other unconfigured. Otherwise the following message will show up and also blade status may go into a faulty state after a reboot.

   Neighbor table overflow.
   print: 54 messages suppressed
Configuring DHCP

By default, some HP switches have DHCP enabled; check the latest Fabric OS 6.x release notes for a complete list of switches. The 4/256 SAN Director and DC SAN Backbone Director (short name, DC Director) do not support DHCP.

The Fabric OS DHCP client supports the following parameters:

- External Ethernet port IP addresses and subnet masks
- Default gateway IP address

The DHCP client uses a DHCP vendor class identifier that allows DHCP servers to determine that the Discoveries and Requests are coming from a switch. The vendor class identifier is the string “BROCADE” followed by the SWBD model number of the platform. For example, the vendor class identifier for a request from an HP StorageWorks DC Director is “BROCADESWBD62.”

**IMPORTANT:** The client conforms to the latest IETF Draft Standard RFCs for IPv4, IPv6, and DHCP.

Enabling DHCP

Connect the DHCP-enabled switch to the network, power on the switch, and the switch automatically obtains the Ethernet IP address, Ethernet subnet mask, and default gateway address from the DHCP server. The DHCP client can only connect to a DHCP server on the same subnet as the switch. Do not enable DHCP if the DHCP server is not on the same subnet as the switch.

When you disable DHCP after the Ethernet information has been configured releases the current Ethernet network interface settings, including Ethernet IP, Ethernet Subnetmask, and Gateway. The Fibre Channel (FC) IP address and subnet mask is static and is not affected by DHCP; see “Setting static Ethernet addresses” on page 28 for instructions on setting the FC IP address.

To enable DHCP:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `ipaddrset` command.
3. If already set up, skip the Ethernet IP address, Ethernet subnet mask, Fibre Channel IP address and subnet mask prompts by pressing Enter.
4. When you are prompted for DHCP[Off], enable it by entering at the prompt:

```
switch:admin> ipaddrset
Ethernet IP Address [192.168.74.102]:
Ethernet Subnetmask [255.255.255.0]:
Fibre Channel IP Address [220.220.220.2]:
Fibre Channel Subnetmask [255.255.0.0]:
Gateway IP Address [192.168.74.1]:
DHCP [Off]:on
```

Disabling DHCP

When you disable DHCP, enter the static Ethernet IP address and subnet mask of the switch and default gateway address. Otherwise, the Ethernet settings may conflict with other addresses assigned by the DHCP server on the network.

To disable DHCP:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `ipaddrset` command.
3. Enter the network information in dotted decimal notation for the Ethernet IP address, Ethernet Subnetmask, and Gateway Address at the prompts. If a static Ethernet address is not available when you disable DHCP, enter 0.0.0.0 at the Ethernet IP address prompt. Skip Fibre Channel prompts by pressing Enter.
4. When you are prompted for DHCP[On], disable it by entering `off`.

   switch:admin> ipaddrset
   Ethernet IP Address [192.168.74.102]:
   Ethernet Subnetmask [255.255.255.0]:
   Fibre Channel IP Address [220.220.220.2]:
   Fibre Channel Subnetmask [255.255.0.0]:
   Gateway IP Address [192.168.74.1]:
   DHCP [On]:off

**Setting the date and time**

Switches maintain the current date and time inside a battery-backed real-time clock (RTC) circuit. Date and time are used for logging events. Switch operation does not depend on the date and time; a switch with an incorrect date and time value still functions properly. However, because the date and time are used for logging, error detection, and troubleshooting, you should set them correctly.

Authorization access to set or change the date and time for a switch is role-based. For an understanding of role-based access, refer to “Using Role-Based Access Control (RBAC)” on page 56.

**IMPORTANT:** If you are running a Fabric OS version earlier than 6.x and secure mode is not enabled, a change in date or time to one switch is forwarded to the principal switch and distributed to the fabric. If secure mode is enabled, date or time changes can be made only on the primary FCS switch and distributed to the fabric.

To set the date and time:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `date` command, using the following syntax:

   `date "mmdHHMMyy"`

   The values represent the following:

   - **mm** is the month; valid values are 01 through 12.
   - **dd** is the date; valid values are 01 through 31.
   - **HH** is the hour; valid values are 00 through 23.
   - **MM** is minutes; valid values are 00 through 59.
   - **yy** is the year; valid values are 00 through 99 (values greater than 69 are interpreted as 1970 through 1999, and values less than 70 are interpreted as 2000-2069).

   ```
   switch:admin> date
   Fri Sep 29 17:01:48 UTC 2007
   switch:admin> date "0927123007"
   Thu Sep 27 12:30:00 UTC 2007
   switch:admin> 
   ```

   For details about how to change time zones, see the `tsTimeZone` command in the *Fabric OS Command Reference*.

**Setting time zones**

You can set the time zone for a switch by name. You can specify the setting using country and city or time zone parameters. Switch operation does not depend on a date and time setting. However, having an accurate time setting is needed for accurate logging and audit tracking.

If the time zone is not set with the new options, the switch retains the offset time zone settings. The `tsTimeZone` command includes an option to revert to the prior time zone format. For more information about the `--old` option, see the *Fabric OS Command Reference*. 
**IMPORTANT:** If you are downgrading to a Fabric OS version earlier than 6.x, or retaining the offset format, see prior versions of the Fabric OS Administrator’s Guide for detailed information about setting time zones using the offset format. See “About the firmware download process” on page 163 for time zone downgrading considerations.

You can set the time zone for a switch using the `tsTimeZone` command. The `tsTimeZone` command allows you to perform the following tasks:

- Display all of the time zones supported in the firmware
- Set the time zone based on a country and city combination or based on a time zone ID such as PST

The time zone setting has the following characteristics:

- Users can view the time zone settings. However, only those with administrative permissions can set the time zones.
- The `tsTimeZone` setting automatically adjusts for Daylight Savings Time.
- Changing the time zone on a switch updates the local time zone setup and is reflected in local time calculations.
- By default, all switches are in the GMT time zone (0,0). If all switches in a fabric are in one time zone, it is possible for you to keep the time zone setup at the default setting.
- System services that have already started will reflect the time zone changes only after the next reboot.
- Time zone settings persist across failover for High Availability.

Setting the time zone on a dual domain Director has the following characteristics:

- Updating the time zone on any switch updates the entire Director.
- The time zone of the entire Director is the time zone of switch 0.

The following procedure describes how to set the time zone for a switch. You must perform the procedure on all switches for which the time zone must be set. However, you only need to set the time zone once on each switch, because the value is written to nonvolatile memory.

To set the time zone:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `tsTimeZone` command as follows:
   ```
   switch:admin> tsTimeZone [--interactive]/[,, timezone_fmt]
   ```
   - Use `tsTimeZone` with no parameters to display the current time zone setting
   - Use `--interactive` to list all of the time zones supported by the firmware.
   - Use `timezone_fmt` to set the time zone by Country/City or by time zone ID, such as PST.

The following example shows how to display the current time zone setup and how to change the time zone to US/Central.

```
switch:admin> tsTimeZone
Time Zone : US/Pacific
switch:admin> tsTimeZone US/Central
switch:admin> tsTimeZone
Time Zone : US/Central
```
The following procedure describes how to set the current time zone using interactive mode to Pacific Standard Time.

To set the time zone interactively:

1. **Type the `tsTimeZone` command as follows:**
   ```
   switch:admin> tstimezone --interactive
   ```

2. **You are prompted to select a general location.**
   Please identify a location so that time zone rules can be set correctly.

3. **Enter the appropriate number or `Ctrl-D` to quit.**

4. **At the prompt, select a country location.**

5. **At the prompt, enter the appropriate number to specify the time zone region or `Ctrl-D` to quit.**

### Synchronizing local time using NTP

You can synchronize the local time of the principal or primary fabric configuration server (FCS) switch to a maximum of eight external network time protocol (NTP) servers. To keep the time in your SAN current, it is recommended that the principal or primary-FCS switch has its time synchronized with at least one external NTP server. The other switches in the fabric will automatically take their time from the principal or primary-FCS switch.

All switches in the fabric maintain the current clock server value in non-volatile memory. By default, this value is the local clock server `<LOCL>` of the principal or primary FCS switch. Changes to the clock server value on the principal or primary FCS switch are propagated to all switches in the fabric.

When a new switch enters the fabric, the time server daemon of the principal or primary FCS switch sends out the addresses of all existing clock servers and the time to the new switch. If a switch with Fabric OS 5.3.0 or later has entered the fabric it will be able to store the list and the active servers; pre-5.3.0 Fabric OS switches will ignore the new list parameter in the payload and will update only the active server address.

If the active NTP server configured is IPv6, then distributing the same in the fabric will not be possible to switches earlier than Fabric OS 5.3.0 because IPv6 is supported for Fabric OS version 5.3.0 and later. The default value LOCL will be distributed to pre-5.3.0 switches.

To synchronize local time with an external source:

1. **Connect to the switch and log in using an account assigned to the admin role.**

2. **Enter the `tsClockServer` command:**
   ```
   switch:admin> tsclockserver "<ntp1;ntp2>"
   ```

   where **ntp1** is the IP address or DNS name of the first NTP server, which the switch must be able to access. The second **ntp2** is the second NTP server and is optional. The operand `"<ntp1;ntp2>"` is optional; by default, this value is LOCL, which uses the local clock of the principal or primary switch as the clock server.

   The `tsclockServer` command accepts multiple server addresses in either IPv4, IPv6, or DNS name formats. When multiple NTP server addresses are passed, `tsclockServer` sets the first obtainable address as the active NTP server. The rest will be stored as backup servers that can take over if the active NTP server fails. The principal or primary FCS switch synchronizes its time with the NTP server every 64 seconds.
   ```
   switch:admin> tsclockserver
   LOCL
   switch:admin> tsclockserver "132.163.135.131"
   ```

   ```
   switch:admin> tsclockserver
   132.163.135.131
   switch:admin>
   ```
The following example shows how to set up more than one NTP server using a DNS name:

```
switch:admin> tsclockserver "10.32.170.1;10.32.170.2;ntp.localdomain.net"
Updating Clock Server configuration...done.
Updated with the NTP servers
```

Changes to the clock server value on the principal or primary FCS switch are propagated to all switches in the fabric.

**Customizing switch names**

Switches can be identified by IP address, Domain ID, World Wide Name (WWN), or by customized switch names that are unique and meaningful.

Switch names can be from 1 to 15 characters long, must begin with a letter, and can contain letters, numbers, or the underscore character. It is not necessary to use quotation marks.

**NOTE:** Changing the switch name causes a domain address format RSCN (registered state change notification) to be issued and may be disruptive to the fabric.

To customize the switch name:

1. Open a Telnet session for each logical switch and enter the `switchName` command.
2. Connect to the switch and log in using an admin account.
3. Enter the `switchName` command, using the following syntax:
   
   `switchname "newname"`
   
   where `newname` is the new name for the switch.
4. Record the new switch name for future reference.
5. Record the new switch name for the second domain for future reference.

**Working with Domain IDs**

Although Domain IDs are assigned dynamically when a switch is enabled, you can reset them manually so that you can control the ID number or resolve a Domain ID conflict when you merge fabrics.

If a switch has a Domain ID when it is enabled, and that Domain ID conflicts with a switch in the fabric, the conflict is automatically resolved. The process can take several seconds, during which time traffic is delayed.

The default Domain ID for HP switches is 1.

**NOTE:** Do not use Domain ID 0. The use of this Domain ID can cause the switch to reboot continuously. Avoid changing the Domain ID on the FCS in secure mode. To minimize down time, change the Domain IDs on the other switches in the fabric.

To display Domain IDs:

1. Connect to a switch and log in as admin.
2. Enter the `fabricShow` command.

Fabric information is displayed, including the Domain ID (D_ID).

```
switch:admin> fabricshow
          Switch ID Worldwide Name    Enet IP Addr    FC IP Addr      Name
---------------------------------------------
64: ffc40 10:00:00:60:69:00:06:56 192.168.64.59 192.168.65.59  "sw5"
65: ffc41 10:00:00:60:69:00:02:0b 192.168.64.180 192.168.65.180  "sw180"
66: ffc42 10:00:00:60:69:00:05:91 192.168.64.60 192.168.65.60  "sw60"
67: ffc43 10:00:00:60:69:10:60:1f 192.168.64.187 0.0.0.0         "sw187"
```
The fields in the **fabricShow** display are:

- **Switch ID** — The switch Domain_ID and embedded port D_ID
- **Worldwide Name** — The switch WWN
- **Enet IP Addr** — The switch Ethernet IP address for IPv4 and IPv6 configured switches. For IPv6 switches, only the static IP address displays
- **FC IP Addr** — The switch FC IP address
- **Name** — The switch symbolic name. An arrow (>) indicates the principal switch.

To set the Domain ID:

1. Connect to the switch and log in using an admin account.
2. Enter the `switchDisable` command to disable the switch.
3. Enter the `configure` command.
4. Enter `y` after the Fabric parameters prompt:
   ```
   Fabric parameters (yes, y, no, n): [no] y
   ```
5. Enter a unique Domain ID at the Domain prompt. Use a Domain ID value from 1 through 239 for normal operating mode (FCSW compatible):
   ```
   Domain: (1..239) [1] 3
   ```
6. Respond to the remaining prompts, or press **Ctrl-D** to accept the other settings and exit.
7. Enter the `switchEnable` command to re-enable the switch.

### Licensed features

You need the following items for each feature that needs to be licensed:

- Transaction key in the paperpack document supplied with the switch software. Or, when you purchased a license, you received a transaction key to use for generating a software license key.
- License ID. To see a switch license ID, issue the `licenseIdShow` command.

Feature licenses may be part of the licensed paperpack supplied with your switch software; if not, you can purchase licenses separately from HP. License keys are provided on a per-product and per-feature basis. Each switch within a fabric will need its own licensing.

**NOTE:** To preserve licenses on your switch, perform a `configupload` prior to upgrading or downgrading your Fabric OS.

If you downgrade your Fabric OS to the version earlier than 6.x, some licenses associated with specific features of Fabric OS 6.x may not work.

Licenses can be associated with a feature version or a blade type.

- If a feature has a version-based license, that license is valid only for a particular version of the feature. If you want a newer version of the feature, you must purchase a new license.
  
  **Version upgrade:** For example, a zoning license that is for Fabric OS version 6.x is added. You can add another zoning license with a version greater than 5.2.0 and above without removing the zoning license for Fabric OS 5.2.0. Upgrading is allowed, but downgrading is not supported.
  
  If a license is not version-based, then it is valid for all versions of the feature.

- If a license is associated with a blade type, the licensed feature can be used only with the associated blade; if you want to use the feature on a second blade, you must purchase an additional license.
Generating a license key

To generate a license key:

1. If you already have a license key, go to “Activating a license key” on page 35 to activate.
   If you do not have a license key, launch an Internet browser and go to:
   http://webkey.external.hp.com/welcome.asp
   The Hewlett-Packard Authorization Center website main menu displays.
2. Click **Generate a license key**.
   The HP StorageWorks Software License Key instruction page opens:

   ![Registration number or product authorization key validation](image)

   3. Enter the information in the required fields.
   4. Follow the onscreen instructions to generate multiple license keys if applicable.
   5. Click **Next**. A verification screen appears.
      Verify that the information is correct. Click **Submit** if the information displayed is correct. If the information is incorrect, click **Previous** and change the information.
   6. Click **Submit**.
   7. An information screen displays the license keys. You also receive an e-mail from the HP licensing company.
   8. Activate the license keys. Go to “Activating a license key” on page 35.

Activating a license key

To activate and verify the license:

1. Connect to the switch and log in using an admin account.
2. Activate the license using the `licenseAdd` command.

   ```bash
   switch:admin> licenseadd "key"
   ```

   The transaction key is case sensitive, so it must be entered exactly as it appears. To lessen the chance of error, copy and paste the transaction key. The quotation marks are optional.

   For 4/256 SAN Director and DC SAN Backbone Director (short name, DC Director) models, licenses are effective on both CP blades, but are valid only when the CP blade is inserted into a Director that has an appropriate license ID stored in the WWN card. If a CP is moved from one Director to another, the license works in the new Director only if the WWN card is the same in the new Director. Otherwise, you must transfer licenses from the old WWN to the new WWN.

   For example, if you swap one CP blade at a time, or replace a single CP blade, then the existing CP blade (the active CP blade) propagates the licenses to the new CP blade.

   If you move a standby CP from one Director to another, then the active CP will propagate its configuration (including license keys).
3. Verify that the license was added by entering the `licenseShow` command. The licensed features currently installed on the switch display. If the feature is not listed, enter the `licenseAdd` command again.

Some features may require additional configuration, or you may need to disable and reenable the switch to make them operational; see the feature documentation for details.

```
switch:admin> licenseshow
RzdeSee9wVlfTu:
    Web license
    Zoning license
    SES license
    Fabric license
    Remote Switch license
    Extended Fabric license
    Fabric Watch license
    Performance Monitor license
    Trunking license
    Security license
    4 Domain Fabric license
    FICON_CUP license
    N Port ID Virtualization license
    High-Performance Extension over FCIP/FC license
    Ports on Demand license - additional 16 port upgrade
    2 Domain Fabric license
    Ports on Demand license - additional 16 port upgrade
```

### Removing a licensed feature

1. Connect to the switch and log in using an admin account.
2. Enter the `licenseShow` command to display the active licenses.
3. Remove the license key using the `licenseRemove` command.
   ```
   switch:admin> licenseremove "key"
   
   The license key is case-sensitive and must be entered exactly as given. The quotation marks are optional. After removing a license key, the optionally licensed feature is disabled when the switch is rebooted or when a switch disable and enable is performed.
   
   4. Enter the `licenseShow` command to verify that the license is disabled.
   ```
   switch:admin> licenseshow
   bQebzbRdScRfc0iK:
       Web license
       Zoning license
   switch:admin> licenseremove "bQebzbRdScRfc0iK"
   removing license key "bQebzbRdScRfc0iK"
   switch:admin>
   ```
   After a reboot (or `switchDisable` and `switchEnable`), only the remaining licenses appear:
   ```
   switch:admin> licenseshow
   SybbzQQ9edTzcc0X:
       Fabric license
   switch:admin>
   ```
   If there are no license keys, `licenseShow` displays “No licenses.”
Features and required licenses

Table 4 lists the licenses that should be installed on the local switch and any connecting switches for a particular feature.

Table 4  License requirements

<table>
<thead>
<tr>
<th>Feature</th>
<th>License</th>
<th>Where license should be installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Domains</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuration up/download</td>
<td>No license required. Configupload or configdownload is a command and comes with the OS on the switch.</td>
<td>n/a</td>
</tr>
<tr>
<td>Diagnostic tools</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Distributed Management Server</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>EX_Ports</td>
<td>Integrated Routing</td>
<td>Local and attached switches.</td>
</tr>
<tr>
<td>FC Fastwrite</td>
<td>FC-IP Services or High Performance Extension over FCIP/FC</td>
<td>Local and attached switches.</td>
</tr>
<tr>
<td>FCIP</td>
<td>FC-IP Services or High Performance Extension over FCIP/FC</td>
<td>Local and attached switches.</td>
</tr>
<tr>
<td>FICON</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>FICON-CUP</td>
<td>FICON Management Server</td>
<td>Local switch.</td>
</tr>
<tr>
<td>FIPS</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Firmware download</td>
<td>No license required. Firmwaredownload is a command and comes with the OS on the switch.</td>
<td>n/a</td>
</tr>
<tr>
<td>Full fabric</td>
<td>Full Fabric</td>
<td>Local switch. May be required on attached switches.</td>
</tr>
<tr>
<td>Ingress rate limiting</td>
<td>Adaptive Networking</td>
<td>Local switch and attached switches.</td>
</tr>
<tr>
<td>Integrated routing</td>
<td>Integrated Routing</td>
<td>Local and attached switches.</td>
</tr>
<tr>
<td>Inter-chassis link (ICL)</td>
<td>ICL</td>
<td>Local and attached ICLs.</td>
</tr>
<tr>
<td>Interoperability</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>IPSec for FCIP tunnels</td>
<td>FC-IP Services or High Performance Extension over FCIP/FC</td>
<td>Local and attached switches.</td>
</tr>
<tr>
<td>LDAP</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Long distance</td>
<td>Extended Fabrics</td>
<td>Local and attached switches.</td>
</tr>
<tr>
<td>NPIV</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Performance monitoring</td>
<td>Basic features - no Advanced features - yes: Advance Performance Monitoring.</td>
<td>Local switch</td>
</tr>
<tr>
<td>Port fencing</td>
<td>Fabric Watch</td>
<td>Local switch</td>
</tr>
</tbody>
</table>
### Table 4  License requirements

<table>
<thead>
<tr>
<th>Feature</th>
<th>License</th>
<th>Where license should be installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Ports on demand licenses. This license applies to a select set of switches.</td>
<td>Local switch</td>
</tr>
<tr>
<td>QoS</td>
<td>Adaptive Networking</td>
<td>Local switch and attached switches.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>RBAC</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Routing traffic</td>
<td>No license required. This includes port-based or exchanged-based routing, static routes, frame-order deliver, and dynamic routes.</td>
<td>n/a</td>
</tr>
<tr>
<td>Security</td>
<td>No license required. Includes the DCC, SCC, FCS, IP Filter, and authentication policies.</td>
<td>n/a</td>
</tr>
<tr>
<td>SNMP</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>SSH public key</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Top Talkers</td>
<td>Advanced Performance Monitoring</td>
<td>Local switch and attached switches.</td>
</tr>
<tr>
<td>Traffic Isolation</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Trunking</td>
<td>ISL Trunking or ISL Trunking Over Extended Fabrics</td>
<td>Local and attached switches.</td>
</tr>
<tr>
<td>Two-factor authentication</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Two-to-four domains in a fabric</td>
<td>Value Line (Two/Four)</td>
<td>Local switch. May be required on attached switches.</td>
</tr>
<tr>
<td>USB usage</td>
<td>No license required.</td>
<td>n/a</td>
</tr>
<tr>
<td>Web Tools</td>
<td>No license required.</td>
<td>Local and any switch you want to manage using Web Tools.</td>
</tr>
<tr>
<td>Zoning</td>
<td>No license required.</td>
<td>Local and attached switches; or any switch you want to use in a zone.</td>
</tr>
</tbody>
</table>

### Inter-Chassis Link (ICL) licensing

ICL ports can be used only with an ICL license. After the addition or removal of a license, the license enforcement is performed on the ICL ports only when the `portdisable` and `portenable` commands are issued on the ports. An ICL license must be installed on both DC Directors forming the ICL connection.
Time-based licenses

A time-based license applies a try-before-you-buy approach to certain features so that you can experience the feature and its capabilities prior to buying the license. Once you have installed the license, you are given a time limit to use the feature. The following lists the types of licenses that have this feature:

- FCIP
- Fabric
- Extended Fabric
- Trunking
- Advanced Performance Monitoring

If you downgrade your switch to a version earlier than 6.x, the time-based license will no longer be available. The license will remain on the switch, but you will not be able to use it.

Once the time-base license is installed you cannot change the time of the switch until the time-based license is removed. You will need to remove the license, change the date, and then reinstall the license on the switch.

High Availability considerations

Whenever license database is modified then it is synchronized with the standby CP. When the active CP is Fabric OS 6.1.0 and has time-based licenses installed, and the standby CP is Fabric OS 6.0.0 or earlier then, upon HA failover the time-based license would no longer be supported on the director or enterprise-class platform. You would not have access to the time-based licensed feature until the CPs Fabric OS 6.1.0 or later. If both CPs have a Fabric OS 6.1.0 or later there will be no change to the time-based licenses or their associated features.

Firmware upgrade and downgrade consideration

When a time-based license is present on the switch, and you downgrade the firmware to Fabric OS 6.0.0 or earlier, then the firmware downgrade will be blocked.

Configupload and Configdownload considerations

The configdownload and configupload commands will download the legacy, enhanced, consumed capacities, and time-based licenses.

Expired licenses

Once a license has expired, you will not be able to view it through the licenseShow command. Expired licenses behave in the same way a license that has been removed from the switch. If your license has expired, you will need to reboot the switch for the expiry to take effect.

Ports on Demand (POD) licensing

**NOTE:** See the hardware reference guide for your switch for the specific POD licensing available.

POD licensing is ready to be unlocked in the switch firmware. Its license key may be part of the licensed paperpack supplied with switch software, or you can purchase the license key separately from HP. You may need to generate a license key from a transaction key supplied with your purchase, see "Generating a license key" on page 35.

Each POD license activates the next group of eight ports in numerical order. For example, the 4/8 SAN Switch or 4/16 SAN Switch activates the first eight with four port increments. Before installing a license key, you must insert transceivers in the ports to be activated. Remember to insert the transceivers in the lowest group of inactive port numbers first.

For example in a SAN Switch 4/32, if only 16 ports are currently active and you are installing one POD license key, make sure to insert the transceivers in ports 16 through 23. If you later install a second license key, insert the transceivers in ports 24 through 31. For details on inserting transceivers, see the switch’s Hardware Reference Manual.
After you install a license key, you must enable the ports to complete their activation. You can do so without disrupting switch operation by issuing the `portEnable` command on each port. Alternatively, you can disable and reenable the switch to activate ports.

**NOTE:** If you enable or disable an active port you will disrupt any traffic and potentially lose data flowing on that port.

If the port is connected to another switch, you will segment the switch from the fabric and all traffic flowing between the disabled port and the fabric will be lost.

### Activating POD

To activate POD:

1. Connect to the switch and log in on an admin account.
2. Optional: To verify the current states of the ports, use the `portShow` command.
   
   In the `portShow` output, the Licensed field indicates whether the port is licensed.
3. Install the Ports on Demand license; see “Enter the information in the required fields.” on page 35.
4. Use the `portEnable` command to enable the ports.
5. Optional: Use the `portShow` command to check the newly activated ports.

If you remove a POD license, the licensed ports will become disabled after the next platform reboot or the next port deactivation.

### Configuring Dynamic Ports on Demand

The Brocade 4Gb SAN Switch for HP c-Class BladeSystem supports blade modules. This switch supports the Dynamic Ports on Demand (DPOD) feature. The Dynamic POD feature automatically assigns POD licenses from a pool of available licenses based on the server blade installation.

#### How ports are assigned to licenses

The Dynamic POD feature detects and assigns ports to a POD license only if the server blade is installed with an HBA present. A server blade that does not have a functioning HBA is treated as an inactive link during initial POD port assignment.

The Dynamic POD feature assigns the ports to the POD license as they come online. Typically, assignments are sequential, starting with the lowest port number. However, variations in the equipment attached to the ports can cause the ports to take different amounts of time to come online. This means that the port assignment order is not guaranteed.

If the switch detects more active links than allowed by the current POD licenses, then some ports will not be assigned a POD license. Ports that do not receive a POD assignment show No Sync or In Sync status; these ports are not allowed to progress to the online state. Ports that cannot be brought online because of insufficient POD licenses show a (No POD License) Disabled status. (Use the `switchShow` command to display the port states.)

To allocate licenses to a specific port instead of automatically assigning them as the ports come online, reserve a license for the port using the `licensePort` command described in “Managing POD licenses” on page 42. The port receives a POD assignment if any are available.

After a port is assigned to the POD set, the port is licensed until it is manually removed from the POD port set using the `licensePort --release` command. When a port is released from its POD port set (Base, Single, or Double), it creates a vacancy in that port set.
Displaying the port license assignment

Use the licensePort --show command to display the available licenses, the current port assignment of those licenses, and the POD method state (dynamic or static).

To display the port licenses:

1. Connect to the switch and log in using an admin account.
2. Enter the licensePort --show command.

```
switch:admin> licenseport --show
24 ports are available in this switch
  Full POD license is installed
  Static POD method is in use
24 port assignments are provisioned for use in this switch:
  12 port assignments are provisioned by the base switch license
  12 port assignments are provisioned by a full POD license
24 ports are assigned to installed licenses:
  12 ports are assigned to the base switch license
  12 ports are assigned to the full POD license
Ports assigned to the base switch license:
  1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20
Ports assigned to the full POD license:
  0, 9, 10, 11, 12, 13, 14, 15, 16, 21, 22, 23
```

The example above shows output from a switch that manually assigned POD licenses.

Activating Dynamic Ports on Demand

If the switch is in the Static POD mode, then activating the Dynamic POD will erase any prior port license assignments the next time the switch is rebooted. The static POD assignments become the initial Dynamic POD assignments. After the Dynamic POD feature is enabled, you can customize the POD license associations.

IMPORTANT: The Dynamic POD feature is supported on the Brocade 4Gb SAN Switch for HP c-Class BladeSystem only.

To enable Dynamic Ports on Demand:

1. Connect to the switch and log in using an admin account.
2. Enter the licensePort --method command with the dynamic option to change the license assignment method to dynamic.

```
switch:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect.
```
3. Enter the reboot command to restart the switch.

```
switch:admin> reboot
```
4. Enter the licensePort --show command to verify that the switch started the Dynamic POD feature.

```
switch:admin> licenseport --show
24 ports are available in this switch
  Full POD license is installed
  Dynamic POD method is in use
24 port assignments are provisioned for use in this switch:
  12 port assignments are provisioned by the base switch license
  12 port assignments are provisioned by a full POD license
  8 ports are assigned to installed licenses:
    8 ports are assigned to the base switch license
    0 ports are assigned to the full POD license
Ports assigned to the base switch license:
```

Disabling Dynamic Ports on Demand

Disabling the Dynamic POD feature (changing the POD method to static), erases any prior port license associations or assignments the next time the switch is rebooted.

To disable Dynamic Ports on Demand:

1. Connect to the switch and log in using an admin account.
2. Enter the `licensePort --method` command with the `static` option to change the license assignment method to static.
   
   switch:admin> licensePort --method static
   
   The POD method has been changed to static.
   
   Please reboot the switch now for this change to take effect.
3. Enter the `reboot` command to restart the switch.
   
   switch:admin> reboot
4. Enter the `licensePort --show` command to verify the switch started the Static POD feature.
   
   switch:admin> licensePort --show
   
   24 ports are available in this switch
   
   Full POD license is installed
   
   Static POD method is in use
   
   24 port assignments are provisioned for use in this switch:
   
   12 port assignments are provisioned by the base switch license
   
   12 port assignments are provisioned by a full POD license
   
   24 ports are assigned to installed licenses:
   
   12 ports are assigned to the base switch license
   
   12 ports are assigned to the full POD license
   
   Ports assigned to the base switch license:
   
   1, 2, 3, 4, 5, 6, 7, 8, 17, 18, 19, 20
   
   Ports assigned to the full POD license:
   
   0, 9, 10, 11, 12, 13, 14, 15, 16, 21, 22, 23

Managing POD licenses

This section explains how to allocate licenses by reserving and releasing POD assignments to specific ports. Disabled ports are not candidates for automatic license assignment by the Dynamic POD feature.

Persistently disable an otherwise viable port to prevent it from coming online, and thereby preserve a license assignment for another port.

Before you can re-assign a license, you must disable the port and release the license.

Reserving a license

Reserving a license for a port assigns a POD license to that port whether the port is online or offline. That license will not be available to other ports that come online before the specified port.

To reserve a port license:

1. Connect to the switch and log in using an admin account.
2. Enter the `licensePort --show` command to verify that there are port reservations still available.
   
   switch:admin> licensePort --show
   
   24 ports are available in this switch
   
   Full POD license is installed
   
   Dynamic POD method is in use
   
   24 port assignments are provisioned for use in this switch:
   
   12 port assignments are provisioned by the base switch license
   
   12 port assignments are provisioned by the full POD license
12 port assignments are provisioned by a full POD license
10 ports are assigned to installed licenses:
10 ports are assigned to the base switch license
0 ports are assigned to the full POD license
Ports assigned to the base switch license:
1*, 2*, 3*, 4*, 5*, 6*, 8*, 21, 22, 23
Ports assigned to the full POD license:
None
Ports not assigned to a license:
0, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

3. If a port reservation is available, then issue the licensePort --reserve command to reserve a license for the port.
   switch:admin> licensePort --reserve 0

4. If all port reservations are assigned, select a port to release its POD license. You must disable the port first by entering the command portdisable <port num>.
   switch:admin>

5. Enter the licensePort --release command to remove the port from the POD license.
   switch:admin> licensePort --release 0

6. Enter the licensePort --show command to verify there is an available port reservation.
   switch:admin> licensePort --show
   24 ports are available in this switch
   Full POD license is installed
   Dynamic POD method is in use
   24 port assignments are provisioned for use in this switch:
   12 port assignments are provisioned by the base switch license
   12 port assignments are provisioned by a full POD license
   10 ports are assigned to installed licenses:
   10 ports are assigned to the base switch license
   0 ports are assigned to the full POD license
   Ports assigned to the base switch license:
   1*, 2*, 3*, 4*, 5*, 6*, 8*, 21, 22, 23
   Ports assigned to the full POD license:
   None
   Ports not assigned to a license:
   0, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

7. Enter the switchEnable command to bring the switch back online.
   switch:admin> switchEnable

Releasing a port

Releasing a port removes it from the POD set; the port will appear as unassigned until it comes back online. Persistently disabling the port will ensure that the port cannot come back online and be automatically assigned to a POD assignment.

To release a port from a POD set:

1. Connect to the switch and log in using an admin account.
2. Enter the switchDisable command to take the switch offline.
   switch:admin> switchDisable
3. Enter the switchShow command to verify the switch state is offline.
4. Enter the licensePort --release command to remove the port from the POD license.
   switch:admin> licensePort --release 0
5. Enter the licensePort --show command to verify the port is no longer assigned to a POD set.
   switch:admin> licensePort --show
   24 ports are available in this switch
   Full POD license is installed
   Dynamic POD method is in use
   24 port assignments are provisioned for use in this switch:
   12 port assignments are provisioned by the base switch license
   12 port assignments are provisioned by a full POD license
   10 ports are assigned to installed licenses:
   10 ports are assigned to the base switch license
   0 ports are assigned to the full POD license
   Ports assigned to the base switch license:
   None
   Ports not assigned to a license:
   0, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20
Ports assigned to the base switch license:
1*, 2*, 3*, 4*, 5*, 6*, 8*, 21, 22, 23
Ports assigned to the full POD license:
None
Ports not assigned to a license:
0, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20

6. Enter the `switchEnable` command to bring the switch back online.
7. Enter the `switchShow` command to verify the switch state is now online.

Disabling and enabling switches

By default, the switch is enabled after power is applied and diagnostics and switch initialization routines have finished. You can disable and reenable it as necessary.

To disable a switch:
1. Connect to the switch and log in using an admin account.
2. Enter the `switchDisable` command.
   All Fibre Channel ports on the switch are taken offline. If the switch was part of a fabric, the fabric is reconfigured.

To enable a switch:
1. Connect to the switch and log in using an admin account.
2. Enter the `switchEnable` command.
   All Fibre Channel ports that passed the POST test are enabled. If the switch has interswitch links (ISLs) to a fabric, it joins the fabric.

Disabling and enabling ports

By default, all licensed ports are enabled. You can disable and reenable them as necessary. Ports that you activate with Ports on Demand must be enabled explicitly, as described in “Activating ports on demand” on page 37.

⚠️ **WARNING!** The fabric will be reconfigured if the port you are enabling or disabling is connected to another switch.

The switch whose port has been disabled will be segmented from the fabric and all traffic flowing between it and the fabric will be lost.

To disable a port:
1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the following command:
   ```
   switch:admin> portdisable portnumber
   ```
   where `portnumber` is the port number of the port you want to disable.

   **For 4/256 SAN Director and DC SAN Backbone Director (short name, DC Director):** Enter the following command:
   ```
   switch:admin> portdisable slotnumber/portnumber
   ```
   where `slotnumber` and `portnumber` are the slot and port numbers of the port you want to disable.

To enable a port:
1. Connect to the switch and log in using an admin account.
2. Enter the following command:
   ```
   switch:admin> portenable portnumber
   ```
   where `portnumber` is the port number of the port you want to enable.
For 4/256 SAN Director and DC Director: Enter the following command:

```
switch:admin> portenable slotnumber/portnumber
```

where `slotnumber` and `portnumber` are the slot and port numbers of the port you want to enable.

(Slots are numbered 1 through 4 and 7 through 10, counting from left to right.)

If the port is connected to another switch, the fabric may be reconfigured. If the port is connected to one or more devices, these devices become available to the fabric.

If you change port configurations during a switch failover, the ports may become disabled. To bring the ports online, re-issue the `portEnable` command after the failover is complete.

### Making basic connections

You can make basic connections to devices and to other switches.

Before connecting a switch to a fabric that contains switches running different firmware versions, you must first set the same PID format on all switches. The presence of different PID formats in a fabric causes fabric segmentation.

- For information on PID formats and related procedures, see “Selecting a PID format” on page 465.
- For information on configuring the routing of connections, see “Routing traffic” on page 205.
- For information on configuring extended interswitch connections, see “Administering Extended Fabrics” on page 361.

### Connecting to devices

To minimize port logins, power off all devices before connecting them to the switch. For devices that cannot be powered off, first use the `portDisable` command to disable the port on the switch, and then connect the device. When powering the devices back on, wait for each device to complete the fabric login before powering on the next one.

### Connecting to other switches

See the hardware reference guide for your specific switch for interswitch link (ISL) connection and cable management information. The standard or default ISL mode is L0. ISL Mode L0 is a static mode, with the following maximum ISL distances:

- 10 km at 1 Gbps
- 5 km at 2 Gbps
- 2.5 km at 4 Gbps
- 1.25 km at 8 Gbps

ISL mode L0 is available on all Fabric OS releases. When you upgrade from Fabric OS 5.3.0 to Fabric 6.x or later, all extended ISL ports are set automatically to L0 mode.

For information on extended ISL modes, which enable longer distance interswitch links, see “Administering Extended Fabrics” on page 361.

### Linking through a gateway

A gateway merges SANs into a single fabric by establishing point-to-point E_Port connectivity between two Fibre Channel switches that are separated by a network with a protocol such as IP or SONET.

Except for link initialization, gateways are transparent to switches; the gateway simply provides E_Port connectivity from one switch to another.

By default, switch ports initialize links using the Exchange Link Parameters (ELP) mode 1. However, gateways expect initialization with ELP mode 2, also referred to as ISL R_RDY mode. Therefore, to enable two switches to link through a gateway, the ports on both switches must be set for ELP mode 2.
Any number of E_Ports in a fabric can be configured for gateway links, provided the following rules are followed:

- All switches in the fabric must be upgraded to Fabric OS 5.2.0 or later.
- All switches in the fabric are using the core PID format.
- The switches connected to both sides of the gateway are included when determining switch count maximums.
- Extended links (those created using the Extended Fabrics licensed feature) and the security features if you are running a Fabric OS version earlier than 6.x in Secure Fabric OS are not supported through gateway links.

To configure a link through a gateway:

1. If you are not sure if the PID format is consistent across the entire fabric, enter the `configShow` command on all switches to check the PID setting. If necessary, change the PID format on any nonconforming switches, as described in “Configuring the PID format” on page 463.
2. Connect to the switch on one end of the gateway and log in using an admin account.
3. Enter the `portCfgIslMode` command that is appropriate for your hardware model:
   - 4/8 SAN Switch and 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP cClass BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, and 400 Multi-protocol Router:
     ```bash
     portCfgIslMode <port, mode>
     ```
   - Specify a port number. Valid values for port number vary depending on the switch type. The mode operand is required: specify 1 to enable ISL R_RDY mode (gateway link) or specify 0 to disable it.
   - 4/256 SAN Director and DC SAN Backbone Director (short name, DC Director):
     ```bash
     portCfgIslMode <slot/port, mode>
     ```
   - Specify a `slot/port` number pair. Valid values for slot and port number vary depending on the switch type. The mode operand is required: specify 1 to enable ISL R_RDY mode (gateway link) or specify 0 to disable it.
   4. In the following example, slot 2, port 3 is enabled for a gateway link:
     ```bash
     switch:admin> portcfgislmode 2/3, 1
     Committing configuration...done.
     ISL R_RDY Mode is enabled for port 3. Please make sure the PID formats are consistent across the entire fabric.
     switch:admin>
     ```
   5. Repeat the steps for any additional ports that will be connected to the gateway.
   6. Repeat the procedure on the switch at the other end of the gateway.

Checking status

You can check the status of switch operation, High Availability features, and fabric connectivity.

To check switch operation:

1. Connect to the switch and log in using an admin account.
2. Enter the `switchShow` command. This command displays a switch summary and a port summary.
3. Check that the switch and ports are online.
4. Use the `switchStatusShow` command to further check the status of the switch.

High Availability (HA) features provide maximum reliability and nondisruptive replacement of key hardware and software modules.

To verify HA features (Directors only):

1. Connect to the switch using an account with admin role
2. Enter the `chassisShow` command to verify the field replaceable units (FRUs).
3. Enter the `haShow` command to verify that HA is enabled, the heartbeat is up, and that the HA state is synchronized between the active and standby CP blades.

4. Enter the `slotShow` command to display the inventory and the current status of each slot in the system.

To verify fabric connectivity:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `fabricShow` command. This command displays a summary of all the switches in the fabric.

```
switch:admin> fabricshow
Switch ID Worldwide Name Enet IP Addr FC IP Addr Name
----------------------------------------------
64: ffc40 10:00:00:60:69:00:06:56 192.168.64.59 192.168.65.59 "sw5"
65: ffc41 10:00:00:60:69:00:02:0b 192.168.64.180 192.168.65.180 >"sw180"
66: ffc42 10:00:00:60:69:00:05:91 192.168.64.60 192.168.65.60  "sw60"
67: ffc43 10:00:00:60:69:10:60:1f 192.168.64.187 0.0.0.0         "sw187"
```

The Fabric has 4 switches

To verify device connectivity:

1. Connect to the switch and log in using an account assigned to the admin role.
2. **Optional**: Enter the `switchShow` command to verify that devices, hosts, and storage are connected.
3. **Optional**: Enter the `nsShow` command to verify that devices, hosts, and storage have successfully registered with the name server.
4. Enter the `nsAllShow` command to display the 24-bit Fibre Channel addresses of all devices in the fabric.

```
switch:admin> nsallshow
{ 010e00 012fe8 012fef 030500 030b04 030b08 030b17 030b18
  030b1e 030b1f 040000 050000 050200 050700 050800 050de8
  050def 051700 061c00 07la00 073c00 090d00 0a0200 0a07ca
  0a07cb 0a07cd 0a07ce 0a07d1 0a07d2 0a07d3 0a07d4
  0a07d5 0a07d6 0a07d9 0a07da 0a07dc 0a07e0 0a07e1 0a07f0
  0a0f02 0a0f0f 0a0f10 0a0f1b 0a0f1d 0b2700 0b2e00 0b2ef8
  0b2ef0 0f0000 0f0226 0f0233 0f02e4 0f02e8 0f02ef 210e00
  211700 2117fe 211fe8 2c0000 2c0300 611000 6114e8 6114ef
  611600 620800 621026 621036 6210e4 6210ef 621400
  621500 621700 621a00
75 Nx_Ports in the Fabric }
```

The number of devices listed should reflect the number of devices that are connected.

To show switches in Access Gateway mode:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `agShow` command.

```
switch:admin> agshow
Worldwide Name Ports Enet IP Addr Firmware Local/Remote Name
-----------------------------------------------
10:00:00:05:1e:02:1d:b0 16 10.32.53.4 v5.2.1 local ag_01
10:00:00:05:1e:03:4b:e7 24 10.32.60.95  v5.2.1 local ag_02
10:00:00:05:1e:35:a2:58 20 10.32.53.180 v5.2.1 remote ag_03
```

This command displays all the switches in Access Gateway mode in the fabric.
Tracking and controlling switch changes

The track changes feature allows you to keep a record of specific changes that may not be considered switch events, but may provide useful information. The output from the track changes feature is dumped to the system messages log for the switch. Use the `errDump` or `errShow` command to view the log.

Items in the log created from the Track changes feature are labeled TRCK.

Trackable changes are:

- Successful login
- Unsuccessful login
- Logout
- Configuration file change from task
- Track changes on
- Track changes off

An SNMP-TRAP mode can also be enabled (see the `trackChangesHelp` command in the Fabric OS Command Reference).

For troubleshooting information on the track changes feature, see “Inaccurate information in the system message log” on page 320.

To enable the track changes feature:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter this command to enable the track changes feature: `trackChangesSet 1`.
   
   A message displays, verifying that the track changes feature is on:
   
   ```
   switch:admin> trackChangesSet 1
   Committing configuration...done.
   switch:admin>
   ```

3. Use the `errDump` or `errShow` command to view the log.
   
   ```
   2004/08/24-08:45:43, [TRCK-1001], 212,, INFO, ras007, Successful login by user admin.
   ```

To display the status of the track changes feature:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `trackChangesShow` command.

   The status of the track changes feature is displayed as either on or off. The display includes whether or not the track changes feature is configured to send SNMP traps.

   ```
   switch:admin> trackChangesShow
   Track changes status: ON
   Track changes generate SNMP-TRAP: NO
   switch:admin>
   ```
To view the switch status policy threshold values:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `switchStatusPolicyShow` command.

   Whenever there is a switch change, an error message is logged and an SNMP `connUnitStatusChange` trap is sent.

   The output is similar to the following:

   ```
   switch:admin> switchstatuspolicyshow
   The current overall switch status policy parameters:
      Down  Marginal
    -------------------------
    PowerSupplies  3         0
    Temperatures  2         1
      Fans  2         1
      WWN  0         1
      CP    0         1
      Blade  0         1
      Flash  0         1
    MarginalPorts  2         1
    FaultyPorts  2         1
      MissingSFPs  0         0
   ```

   The policy parameter determines the number of failed or inoperable units for each contributor that will trigger a status change in the switch.

   Each parameter can be adjusted so that a specific threshold must be reached before that parameter changes the overall status of a switch to MARGINAL or DOWN. For example, if the `FaultyPorts` DOWN parameter is set to 3, the status of the switch will change if 3 ports fail. Only one policy parameter needs to pass the MARGINAL or DOWN threshold to change the overall status of the switch.

   For more information about setting policy parameters, see the Fabric Watch Administrator's Guide.

To set the switch status policy threshold values:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `switchStatusPolicySet` command.

   The current switch status policy parameter values are displayed. You are prompted to enter values for each DOWN and MARGINAL threshold parameter.

   By setting the DOWN and MARGINAL values for a parameter to 0,0 that parameter is no longer used in setting the overall status for the switch.
3. Verify the threshold settings you have configured for each parameter.

Enter the switchStatusPolicyShow command to view your current switch status policy configuration.

**HP StorageWorks 4/8 SAN Switch and 4/16 SAN Switch, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP c-Class BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router:**

```
switch:admin> switchstatuspolicyset
To change the overall switch status policy parameters

The current overall switch status policy parameters:

<table>
<thead>
<tr>
<th>Down</th>
<th>Marginal</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerSupplies     2</td>
<td>1</td>
</tr>
<tr>
<td>Temperatures      2</td>
<td>1</td>
</tr>
<tr>
<td>Fans             2</td>
<td>1</td>
</tr>
<tr>
<td>Flash            0</td>
<td>1</td>
</tr>
<tr>
<td>MarginalPorts   2</td>
<td>1</td>
</tr>
<tr>
<td>FaultyPorts     2</td>
<td>1</td>
</tr>
<tr>
<td>MissingSFPs    0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Note that the value, 0, for a parameter, means that it is NOT used in the calculation.

** In addition, if the range of settable values in the prompt is (0..0), **
** the policy parameter is NOT applicable to the switch. **
** Simply hit the Return key.

Bad PowerSupplies contributing to DOWN status: (0..2) [2] 0
Bad PowerSupplies contributing to MARGINAL status: (0..2) [1] 0
Bad Temperatures contributing to DOWN status: (0..6) [2] 0
Bad Temperatures contributing to MARGINAL status: (0..6) [1] 0
Bad Fans contributing to DOWN status: (0..3) [2] 0
Bad Fans contributing to MARGINAL status: (0..3) [1] 0
Out of range Flash contributing to DOWN status: (0..1) [0] 0
Out of range Flash contributing to MARGINAL status: (0..1) [1] 0
MarginalPorts contributing to DOWN status: (0..32) [2] 0
MarginalPorts contributing to MARGINAL status: (0..32) [1] 0
FaultyPorts contributing to DOWN status: (0..32) [2] 0
FaultyPorts contributing to MARGINAL status: (0..32) [1] 0
MissingSFPs contributing to DOWN status: (0..32) [0] 0
MissingSFPs contributing to MARGINAL status: (0..32) [0] 0

Policy parameter set has been changed
rint12:admin>
```

**4/256 SAN Director and DC SAN Backbone Director (short name, DC Director):** Command output includes parameters related to CP blades.

### Configuring the audit log

When managing SANs, you may want to filter, or audit certain classes of events to ensure that you can view and generate an audit log for what is happening on a switch, particularly for security-related event changes if you are running a Fabric OS version earlier than 6.x. These events include login failures, zone configuration changes, firmware downloads, and other configuration changes—in other words—critical changes that have a serious effect on the operation and security of the switch.

Important information related to event classes is also tracked and made available. For example, you can track changes from an external source by the user name, IP address, or type of management interface used to access the switch.

Auditible events are generated by the switch and streamed to an external host through a configured system message log daemon (syslog). You specify a filter on the output to select the event classes that are sent through the system message log. The filtered events are streamed chronologically and sent to the system message log on an external host in the specified audit message format. This ensures that they can
be easily distinguished from other system message log events that occur in the network. Then, at some regular interval of your choosing, you can review the audit events to look for unexpected changes.

Before you configure audit event logging, familiarize yourself with the following audit event log behaviors and limitations:

- By default, all event classes are configured for audit; to create an audit event log for specific events, you must explicitly set a filter with the class operand and then enable it.
- Audited events are generated specific to a switch and have no negative impact on performance.
- If you are running Fabric OS versions earlier than 6.x, all Secure Fabric OS events are audited.
- Events are not persistently stored on the switch but are streamed to a system message log.
- The audit log depends on the system message log facility and IP network to send messages from the switch to a remote host. Because the audit event log configuration has no control over these facilities, audit events can be lost if the system message log and IP network facilities fail.
- If too many events are generated by the switch, the system message log will become a bottleneck and audit events will be dropped by the Fabric OS.
- If the user name, IP address, or user interface is not transported, an audit message is logged by adding the message None to each of the respective fields.
- For High Availability, the audit event logs exist independently on both active and standby CPs. The configuration changes that occur on the active CP are propagated to the standby CP and take effect.
- Audit log configuration is updated through a configuration download.

See the Fabric OS Command Reference for more information about the auditCfg command and command syntax.

**Auditable event classes**

You configure the audit log using the auditCfg command. Before configuring an audit log, you must select the event classes you want audited. When enabled, the audit log feature audits any RASLog messages (system message log) previously tagged as AUDIT in Fabric OS 6.x. The audit log includes:

- SEC-3001 through SEC-3017
- SEC-3024 through SEC-3029
- ZONE-3001 through ZONE-3012

Table 5 identifies auditable event classes and auditCfg operands used to enable auditing of a specific class.

**Table 5 Auditevent class operands**

<table>
<thead>
<tr>
<th>Operand</th>
<th>Event class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Zone</td>
<td>Audit zone event configuration changes, but not the actual values that were changed. For example, a message may state, “Zone configuration has changed,” but the syslog does not display the actual values that were changed.</td>
</tr>
<tr>
<td>2</td>
<td>Security</td>
<td>Audit any user-initiated security events for all management interfaces. For events that have an impact on an entire fabric, an audit is generated only for the switch from which the event was initiated.</td>
</tr>
<tr>
<td>3</td>
<td>Configuration</td>
<td>Audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.</td>
</tr>
<tr>
<td>4</td>
<td>Firmware</td>
<td>Audit firmware download start, firmware complete, and any other errors encountered during a firmware download.</td>
</tr>
<tr>
<td>5</td>
<td>Fabric</td>
<td>Audit administrative domain-related changes.</td>
</tr>
</tbody>
</table>
NOTE: Only the active CP can generate audit messages because event classes being audited occur only on the active CP. Audit messages cannot originate from other blades in a Director.

Audit events have the following message format:

AUDIT, <Timestamp>, [<Event ID>], <Severity>, <Event Class>, <User ID>/<Role>/<IP address>/<Interface>,<Admin Domain>/<Switch name>,<Reserved>,<Event-specific information>

Switch names are logged for switch components and Director names for Director components. For example, a Director name may be FWDL or RAS and a switch component name may be zone, name server, or SNMP.

Pushed messages contain the administration domain of the entity that generated the event. See the Fabric OS Message Reference for details on message formats. See “Working with Diagnostic Features” on page 285 for details on setting up the system error log daemon.

Audit logging assumes that your syslog is operational and running. Before configuring an audit log, you must perform the following steps to ensure that the host syslog is operational.

To verify host syslog prior to configuring the audit log:

1. Set up an external host machine with a system message log daemon running to receive the audit events that will be generated.
2. On the switch where the audit configuration is enabled, enter the syslogdipaddrAdd command to add the IP address of the host machine so that it can receive the audit events.
   
   You can use IPv4, IPv6, or DNS names for the syslogdipaddrAdd command.
3. Ensure the network is configured with a network connection between the switch and the remote host.
4. Check the host SYSLOG configuration. If all error levels are not configured, you may not see some of the audit messages.

To configure an audit log for specific event classes:

1. Connect to the switch from which you wish to generate an audit log and log in using an account assigned to the admin role.
2. Enter the auditCfg --class command, which defines the specific event classes to be filtered.

   switch:admin> auditcfg --class 2,4
   
   Audit filter is configured.

   The auditCfg event class operands are identified in Table 5.
3. Enter the auditCfg --enable command, which enables audit event logging based on the classes configured in step 2.

   switch:admin> auditcfg --enable
   
   Audit filter is enabled.

   To disable an audit event configuration, enter the auditCfg --disable command.
4. Enter the auditCfg --show command to view the filter configuration and confirm that the correct event classes are being audited, and the correct filter state appears (enabled or disabled).

   switch:admin> auditcfg --show
   
   Audit filter is enabled.
   2=SECURITY
   4=FIRMWARE

5. To verify the audit event log setup, make a change affecting an enabled event class, and confirm that the remote host machine receives the audit event messages.

   The following example shows the SYSLOG (system message log) output for audit logging.

   Jun 2 08:33:04 [10.32.220.7.2.2] raslogd: AUDIT, 2006/06/02-15:25:53, [SULB-1003], INFO, FIRMWARE, root/root/NONE/console/CLI, ad_0/ras007_chassis, , Firmwarecommit has started.
   Jun 5 06:45:33 [10.32.220.70.2.2] raslogd: AUDIT, 2006/06/05-13:38:17, [CONF-1010], INFO, CONFIGURATION, root/root/NONE/console/CLI, ad_0/ras070, , configDownload failed
Shutting down switches and Directors

To avoid corrupting your file system, HP recommends that you perform graceful shutdowns of switches and Directors. The following procedure describes how to gracefully shut down a switch.

To power off a switch:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `sysShutdown` command.
3. At the prompt, enter `y`.

   switch:admin> sysshutdown
   This command will shutdown the operating systems on your switch.
   You are required to power-cycle the switch in order to restore operation.
   Are you sure you want to shutdown the switch [y/n]: y

4. Wait until the following message displays:

   Broadcast message from root (ttyS0) Wed Jan 25 16:12:09 2006...
   The system is going down for system halt NOW !!
   INIT: Switching to runlevel: 0
   INIT: Sending processes the TERM signal
  Unmounting all filesystems.
The system is halted
flushing ide devices: hda
Power down.

5. Power off the switch.

To power off a Director:

1. From the active CP in a dual CP platform, enter the `sysShutdown` command.

   When the `sysShutdown` command is issued on the active CP, the active CP, the standby CP, and any AP blades are all shut down.

2. At the prompt, enter `y`.

3. Wait until you see the following message:

   Broadcast message from root (ttyS0) Wed Jan 25 17:01:41 2006...
   The system is going down for system halt NOW !!
   INIT: Switching to runlevel: 0
   INIT: Sending processes the TERM signal
   Unmounting all filesystems.
The system is halted
flushing ide devices: hda
Power down.

4. Power off the switch.

High Availability of daemon processes

Fabric OS 6.x supports automatic restart of non-critical daemons. Starting these non-critical daemons is automatic, you cannot configure the startup process. The following sequence of events occurs when a non-critical daemon fails:

1. When a non-critical daemon fails or dies, a RASLog and AUDIT event message is logged.
2. The daemon is automatically started again.
3. If the restart is successful, then another message is sent to RASLog and AUDIT reporting the successful restart status.
4. If the restart fails, another message is sent to RASLog and no further attempts are made to restart the daemon.
Schedule downtime and reboot the switch at your convenience. Table 6 lists the daemons that are considered non-critical and are automatically restarted on failure.

**Table 6  Daemons that are automatically restarted**

<table>
<thead>
<tr>
<th>Daemon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arrd</td>
<td>Asynchronous Response Router (used to send management data to hosts when the switch is accessed through the APIs (FA API or SMI-S)).</td>
</tr>
<tr>
<td>Cald</td>
<td>Common Access Layer Daemon (used by Manageability Applications).</td>
</tr>
<tr>
<td>Evmd</td>
<td>Event Monitor Daemon (used by port and switch SCNs, firmwareDownload, and configDownload)</td>
</tr>
<tr>
<td>Raslogd</td>
<td>Remote Access Service Log Daemon logs error detection, reporting, handling, and presentation of data into a format readable by management tools and the user.</td>
</tr>
<tr>
<td>Rpcd</td>
<td>Remote Procedure Call daemon used by the API (Fabric Access API and SMI-S).</td>
</tr>
<tr>
<td>Snmpd</td>
<td>Simple Network Management Protocol Daemon.</td>
</tr>
<tr>
<td>Traced</td>
<td>Trace Daemon. Provides trace entry date/time translation to Trace Device at startup and when date/time changed by command. Maintains the trace dump trigger parameters in a Trace Device. Performs the trace Background Dump, trace automatic FTP, and FTP “aliveness check” if auto-FTP is enabled.</td>
</tr>
<tr>
<td>Trackd</td>
<td>Track Changes Daemon.</td>
</tr>
<tr>
<td>Webd</td>
<td>Webserver daemon used for Web Tools (includes httpd as well).</td>
</tr>
</tbody>
</table>
2 Managing user accounts

This chapter provides information and procedures on managing authentication and user accounts for the switch management channel.

Overview

In addition to the default accounts—root, factory, admin, and user—Fabric OS supports up to 252 additional user-defined accounts in each logical switch (domain). These accounts expand your ability to track account access and audit administrative activities.

Each user-defined account is associated with the following:

- **Admin Domain list**—Specifies what Admin Domains a user account is allowed to log in to.
- **Home Admin Domain**—Specifies the Admin Domain that the user is logged in to by default. The home Admin Domain must be a member of the user’s Admin Domain list.
- **Role**—Determines functional access levels within the bounds of the user’s current Admin Domain.

Fabric OS provides three options for authenticating users—remote RADIUS services, remote LDAP service, and the local switch user database. All options allow users to be centrally managed using the following methods:

- **Remote RADIUS servers**—Users are managed in a remote RADIUS server. All switches in the fabric can be configured to authenticate against the centralized remote database.
- **Remote LDAP servers**—Users are managed in a remote LDAP server. All switches in the fabric can be configured to authenticate against the centralized remote database.
- **Local user database**—Users are managed using the local user database. The local user database is manually synchronized using the `distribute` command to push a copy of the switch’s local user database to all other Fabric OS 5.3.0 and later switches in the fabric.

Accessing the management channel

Table 7 shows the number of simultaneous login sessions allowed for each role. The roles are displayed in alphabetic order which does not reflect their importance.

<table>
<thead>
<tr>
<th>Role name</th>
<th>Maximum sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>2</td>
</tr>
<tr>
<td>BasicSwitchAdmin</td>
<td>4</td>
</tr>
<tr>
<td>FabricAdmin</td>
<td>4</td>
</tr>
<tr>
<td>Operator</td>
<td>4</td>
</tr>
<tr>
<td>SecurityAdmin</td>
<td>4</td>
</tr>
<tr>
<td>SwitchAdmin</td>
<td>4</td>
</tr>
<tr>
<td>User</td>
<td>4</td>
</tr>
<tr>
<td>ZoneAdmin</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 7 Maximum number of simultaneous sessions
Using Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) defines the capabilities that a user account has based on the role the account has been assigned. For each role, there is a set of pre-defined permissions on the jobs and tasks that can be performed on a fabric and its associated fabric elements. Fabric OS 6.x uses RBAC to determine which commands a user can issue.

When you log in to a switch, your user account is associated with a pre-defined role. The role that your account is associated with determines the level of access you have on that switch and in the fabric. Table 8 outlines the Fabric OS predefined roles.

Table 8 Fabric OS 6.x roles

<table>
<thead>
<tr>
<th>Role name</th>
<th>Fabric OS version</th>
<th>Duties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>All</td>
<td>All administration</td>
<td>All administrative commands.</td>
</tr>
<tr>
<td>BasicSwitchAdmin</td>
<td>5.2.0 and later</td>
<td>Restricted switch administration</td>
<td>Mostly monitoring with limited switch (local) commands.</td>
</tr>
<tr>
<td>FabricAdmin</td>
<td>5.2.0 and later</td>
<td>Fabric and switch administration</td>
<td>All switch and fabric commands, excludes user management and Administrative Domains commands.</td>
</tr>
<tr>
<td>Operator</td>
<td>5.2.0 and later</td>
<td>General switch administration</td>
<td>Routine switch maintenance commands.</td>
</tr>
<tr>
<td>SecurityAdmin</td>
<td>5.3.0 and later</td>
<td>Restricts security functions</td>
<td>All switch security and user management functions.</td>
</tr>
<tr>
<td>SwitchAdmin</td>
<td>5.0.0 and later</td>
<td>Local switch administration</td>
<td>Most switch (local) commands, excludes security, user management, and zoning commands.</td>
</tr>
<tr>
<td>User</td>
<td>All</td>
<td>Monitoring only</td>
<td>Nonadministrative use, such as monitoring system activity.</td>
</tr>
<tr>
<td>ZoneAdmin</td>
<td>5.2.0 and later</td>
<td>Zone administration</td>
<td>Zone management commands only.</td>
</tr>
</tbody>
</table>

You can perform these operations only on the primary FCS switch.

For legacy users with no Admin Domain specified, the user will have access to AD 0 through 255 (physical fabric admin) if their current role is Admin; otherwise, the user will have access to AD0 only.

If some Admin Domains have been defined for the user and all of them are inactive, the user will not be allowed to log in to any switch in the fabric.

If no Home Domain is specified for a user, the system provides a default home domain. The default home domain for the predefined account is AD0. For user-defined accounts, the default home domain is the Admin Domain in the user’s Admin Domain list with the lowest ID.
Role permissions

Table 9 describes the types of permissions that are assigned to roles.

Table 9  Permission types

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>O</td>
<td>Observe</td>
<td>The user can run commands using options that display information only, such as running <code>userConfig --show -a</code> to show all users on a switch.</td>
</tr>
<tr>
<td>M</td>
<td>Modify</td>
<td>The user can run commands using options that create, change, and delete objects on the system, such as running <code>userconfig --change username -r rolename</code> to change a user’s role.</td>
</tr>
<tr>
<td>OM</td>
<td>Observe and modify</td>
<td>The user can run commands using both observe and modify options; if a role has modify permissions, it almost always has observe.</td>
</tr>
<tr>
<td>N</td>
<td>None</td>
<td>The user is not allowed to run commands in a given category.</td>
</tr>
</tbody>
</table>

Table 10 shows the permission type for categories of commands that each role is assigned. The permissions apply to all commands within the specified category. For a complete list of commands and role permissions, see the Fabric OS Command Reference.

Table 10  RBAC permissions matrix

<table>
<thead>
<tr>
<th>Category</th>
<th>Role permission</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User</td>
</tr>
<tr>
<td>Admin Domains</td>
<td>N</td>
</tr>
<tr>
<td>Admin Domains—Selection</td>
<td>OM</td>
</tr>
<tr>
<td>Access Gateway</td>
<td>O</td>
</tr>
<tr>
<td>APM</td>
<td>O</td>
</tr>
<tr>
<td>Audit</td>
<td>O</td>
</tr>
<tr>
<td>Authentication</td>
<td>N</td>
</tr>
<tr>
<td>Blade</td>
<td>O</td>
</tr>
<tr>
<td>Chassis Configuration</td>
<td>O</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>N</td>
</tr>
<tr>
<td>Data Migration Manager</td>
<td>N</td>
</tr>
<tr>
<td>Debug</td>
<td>N</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>O</td>
</tr>
<tr>
<td>Ethernet Configuration</td>
<td>O</td>
</tr>
<tr>
<td>Fabric</td>
<td>O</td>
</tr>
<tr>
<td>Fabric Distribution</td>
<td>N</td>
</tr>
<tr>
<td>Fabric Routing</td>
<td>O</td>
</tr>
<tr>
<td>Fabric Watch</td>
<td>O</td>
</tr>
<tr>
<td>FICON</td>
<td>O</td>
</tr>
<tr>
<td>Firmware Management</td>
<td>O</td>
</tr>
<tr>
<td>FRU Management</td>
<td>O</td>
</tr>
</tbody>
</table>
Table 10 RBAC permissions matrix (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Role permission</th>
<th>Switch admin</th>
<th>Zone admin</th>
<th>Fabric admin</th>
<th>Basic switch admin</th>
<th>Admin</th>
<th>Security admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA (High Availability)</td>
<td>O</td>
<td>O</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>iSCSI</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>License</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>LDAP</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>OM</td>
</tr>
<tr>
<td>Local User Environment</td>
<td>OM</td>
<td>OM</td>
<td>OM</td>
<td>OM</td>
<td>OM</td>
<td>OM</td>
<td>OM</td>
</tr>
<tr>
<td>Logging</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Management Access Configuration</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Management Server</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Name Server</td>
<td>O</td>
<td>O</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Nx_Port Management</td>
<td>O</td>
<td>M</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Physical Computer System</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>PKI</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>N</td>
<td>O</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Port Mirroring</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>OM</td>
</tr>
<tr>
<td>QOS</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
</tr>
<tr>
<td>RADIUS</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>OM</td>
</tr>
<tr>
<td>Routing—Advanced</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Routing—Basic</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Security</td>
<td>O</td>
<td>N</td>
<td>O</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Session Management</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>OM</td>
<td>OM</td>
</tr>
<tr>
<td>SNMP</td>
<td>O</td>
<td>O</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Statistics</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Statistics—Device</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Statistics—Port</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Switch Configuration</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Switch Management</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Switch Management—IP Configuration</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>Switch Port Configuration</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>OM</td>
<td>OM</td>
</tr>
<tr>
<td>Switch Port Management</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
</tr>
<tr>
<td>Topology</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>N</td>
<td>OM</td>
<td>O</td>
<td>OM</td>
</tr>
<tr>
<td>User Management</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>OM</td>
</tr>
<tr>
<td>WWN Card</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
<td>N</td>
<td>OM</td>
</tr>
<tr>
<td>Zoning</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>OM</td>
<td>OM</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

Set the authentication model on each switch. Refer to “Authentication model” on page 65 for more information.
Managing the local database user accounts

User add, change, and delete operations are subject to the subset rule: an admin with ADlist 0-10 cannot perform operations on an admin, user, or any role with an ADlist 11-25. The user account being changed must have an ADlist that is a subset of the account that is making the change.

About the default accounts

Fabric OS provides the following predefined accounts in the local switch user database. The password for all default accounts should be changed during the initial installation and configuration for each switch. Table 11 lists default local user accounts.

Table 11  Default local user accounts

<table>
<thead>
<tr>
<th>Account name</th>
<th>Role</th>
<th>Admin domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Admin</td>
<td>AD0-255</td>
<td>Most commands have observe-modify permission.</td>
</tr>
<tr>
<td>factory</td>
<td>Factory</td>
<td>AD0-255</td>
<td>Reserved.</td>
</tr>
<tr>
<td>root</td>
<td>Root</td>
<td>AD0-255</td>
<td>Reserved.</td>
</tr>
<tr>
<td>user</td>
<td>User</td>
<td>AD0</td>
<td>Most commands have observe-only permission.</td>
</tr>
</tbody>
</table>

Defining local user accounts

In addition to the default administrative and user accounts, Fabric OS supports up to 252 user-defined accounts in each logical switch (domain). These accounts expand your ability to track account access and audit administrative activities.

The following procedures can be performed on local user accounts. Administrators can act on other accounts only if that account has an Admin Domain list that is a subset of the administrator.

To display account information:
1. Connect to the switch and log in using an admin account.
2. Enter the appropriate show operands for the account information you want to display:
   - userConfig --show -a to show all account information for a logical switch
   - userConfig --show -b to show all backup account information for a logical switch
   - userConfig --show username to show account information for the specified account
   - userConfig --showad -a admindomain_ID to show all accounts permitted to select the specified admindomain_ID
To create an account:

1. Connect to the switch and log in using an admin account.
2. Enter the following command:

   ```
   userConfig --add <username> -r <rolename> [-h <admindomain_ID>]
   [-a <admindomain_ID_list>] [-d <description>] [-x]
   ```

   - `username` Specifies the account name, which must begin with an alphabetic character. The name can be from 8 to 40 characters long. It is case-sensitive and can contain alphabetic and numeric characters, the period (.) and the underscore (_). It must be different than all other account names on the logical switch. The account name cannot be the same as a role name.

   - `-r rolename` Specifies the role: User, SwitchAdmin, ZoneAdmin, FabricAdmin, BasicSwitchAdmin, Operator, or Admin in nonsecure mode; in secure mode you can also use NonfcsAdmin.

   - `-h admindomain_ID` Optional: Specifies the home Administrative Domain; if no Administrative Domain is specified, then the lowest numbered Administrative Domain in the list is assigned.

   - `-a admindomain_ID_list` Optional: Specifies which Administrative Domains the user may access; if no Administrative Domains are listed, the user is automatically assigned to AD0. Use comma-separated lists, ranges, or both for example -a 0,9,10-1 5,244.

   - `-d description` Optional: Adds a description to the account. The description field can be up to 40 printable ASCII characters long. The following characters are not allowed: asterisk (*), single quotation mark (‘), quotation mark (“), exclamation point (!), semicolon (;), and colon (:).

   - `-x` Specifies an expired password that must be changed the first time the user logs in.

3. In response to the prompt, enter a password for the account.

   The password is not displayed when you enter it on the command line.

To delete an account:

1. Connect to the switch and log in using an admin account.
2. Enter the following command:

   ```
   userConfig --delete username
   ```

   where `username` specifies the account name

   You cannot delete the default accounts. An account cannot delete itself. All active CLI sessions for the deleted account are logged out.

3. At the prompt for confirmation, enter **y**.
To change account parameters:

When changing account parameters, if you change the ADlist for the user account, all of the currently active sessions for that account will be logged out.

1. Connect to the switch and log in using an admin account.
2. Enter the following command:

   ```
   userconfig --change username [-r rolename] [-h admindomain_ID]
   [-a admindomain_ID_list] [-d description] [-e yes | no] -u -x
   ```

   - **username**: Specifies the account for which parameters are being changed.
   - **-r rolename**: Changes the role to one of the names listed in Table 8 on page 54. In secure mode, role can also be changed to nonfcsadmin role. An account cannot change its own role. Account with Admin role can change the role names of all user-defined accounts except those with Admin roles.
   - **-h admindomain_ID**: Optional: Changes the home Administrative Domain; if no Administrative Domain is specified, then the lowest numbered Administrative Domain in the list is assigned.
   - **-a admindomain_ID_list**: Optional: Changes which Administrative Domains the user may access; if no Administrative Domains are listed, the user is automatically assigned to AD0. Use comma-separated lists, ranges, or both for example -a 0,9,10,15,244.
   - **-d description**: Optional: Changes the description to the account. The description field can be up to 40 printable ASCII characters long. The following characters are not allowed: asterisk (*), single quotation mark (‘), quotation mark (“), exclamation point (!), semicolon (;), and colon (:).
   - **-e**: Optional: Enables or disables the account. Enter yes to enable the account or no to disable it. If you disable an account, all active CLI sessions for that account are logged out. You can enable or disable user-defined or default accounts.
   - **-u**: Unlocks the user account.
   - **-x**: Specifies an expired password that must be changed the first time the user logs in.

To add an Administrative Domain to the account:

1. Connect to the switch and log in using an admin account.
2. Enter the following command:

   ```
   userConfig --addad <username> [-h <admindomain_ID>] [-a <admindomain_ID_list>]
   ```

   where `<username>` is the account to which the Administrative Domain is being added (the account must already exist) `<admindomain_ID>` is the home Administrative Domain and `<admindomain_ID_list>` adds the new list Administrative Domain to the existing list.

3. Log into the switch again to verify access to the newly-added Admin Domain.

To remove an Administrative Domain from the account:

When removing an Admin Domain from an account, all of the currently active sessions for that account will be logged out.

1. Connect to the switch and log in using an admin account.
2. Enter the following command:

   ```
   userConfig --deletead <username> [-h <admindomain_ID>] [-a <admindomain_ID_list>]
   ```

   where `<username>` is the account from which the Admin Domain is being removed (the account must already exist) `admindomain_ID` is the home Admin Domain, and `admindomain_ID_list` is the Admin Domain list to be removed from the existing list. If the `-h` argument is not specified, the home Admin Domain will either remain as it was or will be the lowest Admin Domain ID in the remaining list.
Recovering accounts

The following conditions apply to recovering user accounts:

- The attributes in the backup database replace the attributes in the current account database.
- An event is stored in the system message log, indicating that accounts have been recovered.

To recover an account:

1. Connect to the switch and log in using an admin account.
2. If a backup database exists, enter the following command.
   ```
   userConfig --recover
   ```
   The AD list for a user account is not recovered; recovered accounts are given access only to AD0, regardless of previous AD assignments.

Changing local account passwords

The following rules apply to changing passwords:

- Users can change their own passwords.
- Only users with Admin roles can change the password for other accounts. When changing an Admin account password, you must provide the current password.
- An admin with ADlist 0-10 cannot change the password on an admin, user, or any role with an ADlist 11-25. The user account being changed must have an ADlist that is a subset of the account that is making the change.
- A new password must have at least one character different from the old password.
- You cannot change passwords using SNMP.

**NOTE:** Starting with Fabric OS 4.4.0, accounts with the Admin role can use Web Tools to change passwords. Starting with Fabric OS 3.2.0, you cannot change default account names. Starting with Fabric OS 5.1.0 password policies apply.

For information on password behavior when you upgrade (or downgrade) firmware, see "Upgrading and downgrading firmware" on page 166.

To change the password for the current login account:

1. Connect to the switch and log in using an admin account.
2. Enter the following command:
   ```
   passwd
   ```
3. Enter the requested information at the prompts.

To change the password for a different account:

1. Connect to the switch and log in using an admin account.
2. Enter the following command:
   ```
   passwd "name"
   ```
   where name is the name of the account for which the password is being changed.
3. Enter the requested information at the prompts.
Configuring the local user database

This section covers the following topics:

- "Distributing the local user database" on page 61
- "Protecting the local user database from distributions" on page 61
- "Configuring password policies" on page 62

Distributing the local user database

Distributing the local switch user database and passwords to other switches in the fabric causes the distributed database to replace (overwrite) the database on the target switch. The ‘Locked’ status of a user account is not distributed as part of local user database distribution.

When distributing the user database, the database may be rejected for one of the following reasons:

- One of the target switches does not have Fabric OS 5.3.0 or later.
- One of the target switch’s user database is protected.

Distribute the user database and password policies only to Fabric OS 5.2.0 or later switches; the distribution command fails if any of the target switches are an earlier version.

To distribute the local user database:

1. Connect to the switch and log in using an admin account.
2. Enter the following command:
   
   ```
   distribute -p PWD -d <switch_list>
   ```
   
   where `<switch_list>` is a semicolon-separated list of switch Domain IDs, switch names, or switch WWN addresses. You can also specify `-d "*"` to send the local user database only to Fabric OS 5.2.0 or later switches in the fabric.

Protecting the local user database from distributions

Fabric OS 5.2.0 and later allows you to distribute the user database and passwords to other switches in the fabric. When the switch accepts a distributed user database, it replaces the local user database with the user database it receives.

By default, Fabric OS 6.x switches accept the user databases and passwords distributed from other switches. This section explains how to protect the local user database from being overwritten.

To accept distribution of user databases on the local switch:

1. Connect to the switch and log in using an admin account.
2. Enter the following command:
   
   ```
   fddCfg --localaccept PWD
   ```
   
   where `PWD` is the user database policy. Other supported policy databases are SCC, DCC, AUTH, FCS, and IPFILTER.

To reject distributed user databases on the local switch:

1. Connect to the switch and log in using an admin account.
2. Enter the following command:
   
   ```
   fddCfg --localreject PWD
   ```
Configuring password policies

The password policies described in this section apply to the local switch user database only. Configured password policies (and all user account attribute and password state information) are synchronized across CPs and remain unchanged after an HA failover. Password policies can also be manually distributed across the fabric (see “Distributing the local user database” on page 61). Following is a list of the configurable password policies:

- Password strength
- Password history
- Password expiration
- Account lockout

All password policies are enforced during logins to the standby CP. However, you may observe that the password enforcement behavior on the standby CP is inconsistent with prior login activity because password state information from the active CP is automatically synchronized with the standby CP, thereby overwriting any password state information that was previously stored there. Also, password changes are not permitted on the standby CP.

Password authentication policies configured using the `passwdCfg` command are not enforced during initial prompts to change default passwords.

Setting the password strength policy

The password strength policy is enforced across all user accounts, and enforces a set of format rules to which new passwords must adhere. The password strength policy is enforced only when a new password is defined. The total of the other password strength policy parameters (lowercase, uppercase, digits, and punctuation) must be less than or equal to the value of the `MinLength` parameter.

Use the following attributes to set the password strength policy:

- **Lowercase**
  Specifications the minimum number of lowercase alphabetic characters that must appear in the password. The default value is zero. The maximum value must be less than or equal to the `MinLength` value.

- **Uppercase**
  Specifies the minimum number of uppercase alphabetic characters that must appear in the password. The default value is zero. The maximum value must be less than or equal to the `MinLength` value.

- **Digits**
  Specifies the minimum number of numeric digits that must appear in the password. The default value is zero. The maximum value must be less than or equal to the `MinLength` value.

- **Punctuation**
  Specifies the minimum number of punctuation characters that must appear in the password. All printable, non-alphanumeric punctuation characters except colon (:) are allowed. The colon character is not allowed because it is incompatible with Web Tools. The default value is zero. The maximum value must be less than or equal to the `MinLength` value.

- **MinLength**
  Specifies the minimum length of the password. The minimum can be from 8 to 40 characters. New passwords must between the minimum length specified and 40 characters. The default value is 8. The maximum value must be greater than or equal to the `MinLength` value.

- **Repeat**
  Specifies the length of repeated character sequences that will be disallowed. For example, if the "repeat" value is set to 3, a password “passAAAword” is disallowed because it contains the repeated sequence “AAA”. A password of “passAAword” would be allowed because no repeated character sequence exceeds two characters. The range of allowed values is 1 – 40. The default value is 1.
• **Sequence**
  Specifies the length of sequential character sequences that will be disallowed. A sequential character sequence is defined as a character sequence in which the ASCII value of each contiguous character differs by one. The ASCII value for the characters in the sequence must all be increasing or decreasing. For example, if the “sequence” value is set to 3, a password “passABCword” is disallowed because it contains the sequence “ABC”. A password of “passABword” would be allowed because it contains no sequential character sequence exceeding two characters. The range of allowed values is 1 – 40. The default value is 1.

  The following example shows a password strength policy that requires passwords to contain at least three uppercase characters, four lowercase characters and two numeric digits; the minimum length of the password is nine characters.

  `passwdcfg --set -uppercase 3 -lowercase 4 -digits 2 -minlength 9`

**Setting the password history policy**

  The password history policy prevents users from recycling recently used passwords, and is enforced across all user accounts when users are setting their own passwords. The password history policy is enforced only when a new password is defined.

  Specify the number of past password values that are disallowed when setting a new password. Allowable password history values range between 1 and 24. The default value is 2, which means the current password cannot be reused. The value 2 indicates that the current and the two previous passwords cannot be used (and so on, up to 24 passwords).

  This policy does not verify that a new password meets a minimal standard of difference from prior passwords, rather, it only determines whether or not a newly-specified password is identical to one of the specified number (1-24) of previously used passwords.

  The password history policy is not enforced when an administrator sets a password for another user; instead, the user’s password history is preserved and the password set by the administrator is recorded in the user’s password history.

**Setting the password expiration policy**

  The password expiration policy forces expiration of a password after a configurable period of time, and is enforced across all user accounts. A warning that password expiration is approaching is displayed when the user logs in. When a user’s password expires, he or she must change the password to complete the authentication process and open a user session. You can specify the number of days prior to password expiration during which warnings will commence. Password expiration does not disable or lock out the account.

  Use the following attributes to set the password expiration policy:

  • **MinPasswordAge**
    Specifies the minimum number of days that must elapse before a user can change a password. `MinPasswordAge` values range from 0 to 999. The default value is zero. Setting this parameter to a non-zero value discourages users from rapidly changing a password in order to circumvent the password history setting to select a recently-used password. The `MinPasswordAge` policy is not enforced when an administrator changes the password for another user.

  • **MaxPasswordAge**
    Specifies the maximum number of days that can elapse before a password must be changed, and is also known as the password expiration period. `MaxPasswordAge` values in range from 0 to 999. The default value is zero. Setting this parameter to zero disables password expiration.

  • **Warning**
    Specifies the number of days prior to password expiration that a warning about password expiration is displayed. `Warning` values range from 0 to 999. The default value is 0 days. When `MaxPasswordAge` is set to a non-zero value, `MinPasswordAge` and `Warning` must be set to a value that is less than or equal to `MaxPasswordAge`.
Upgrade and downgrade considerations

If you are upgrading from a 5.3.x environment to 6.x, the existing password databases do not contain the state information that implements password expiration. So, when the password expiration policy is first set after an upgrade to 6.x, any user who has not changed their password will have their password expiration period set to the maximum password expiration period. You must explicitly define the password expiration for users who have not performed a password change subsequent to the upgrade.

For example:
- March 1st—Using a 5.3.x Fabric OS release. User A changes their password.
- April 1—Upgrade to 6.x
- May 1—User B changes his password.
- June 1—The password configuration parameter MaxPasswordAge is set to 90 days.

User A’s password will expire on September 1. User B’s password will expire on August 1.

Setting the account lockout policy

The account lockout policy disables a user account when that user exceeds a specified number of failed login attempts, and is enforced across all user accounts. You can configure this policy to keep the account locked until explicit administrative action is taken to unlock it, or the locked account can be automatically unlocked after a specified period. Administrators can unlock a locked account at any time.

A failed login attempt counter is maintained for each user on each switch instance. The counters for all user accounts are reset to zero when the account lockout policy is enabled. The counter for an individual account is reset to zero when the account is unlocked after a LockoutDuration period expires.

The admin account can also have the lockout policy enabled on it. The admin account lockout policy is disabled by default and uses the same lockout threshold as the other roles. It can be automatically unlocked after the lockout duration passes or when it is manually unlocked by either a user account that has a securityAdmin or other Admin role.

- userConfig --change <account name> -u
- passwdCfg --disableadminlockout

Note that the account-locked state is distinct from the account-disabled state.

Use the following attributes to set the account lockout policy:

- LockoutThreshold
  Specifies the number of times a user can attempt to log in using an incorrect password before the account is locked. The number of failed login attempts is counted from the last successful login. LockoutThreshold values range from 0 to 999, and the default value is 0. Setting the value to 0 disables the lockout mechanism.

- LockoutDuration
  Specifies the time, in minutes, after which a previously locked account is automatically unlocked. LockoutDuration values range from 0 to 99999, and the default value is 30. Setting the value to 0 disables lockout duration, and would require a user to seek administrative action to unlock the account. The lockout duration begins with the first login attempt after the LockoutThreshold has been reached. Subsequent failed login attempts do not extend the lockout period.

To enable the admin lockout policy:

1. Log in to the switch using an admin or securityAdmin account.
2. Type passwdCfg --enableadminlockout.

   The policy is now enabled.

To unlock an account:

1. Log in to the switch using an admin or securityAdmin account.
2. Type userConfig --change <account name> -u.

   where <account name> is the name of the user account that is locked out.
To disable the admin lockout policy:

1. Log in to the switch using an admin or securityAdmin account.
2. Type `passwdCfg --disableadminlockout`.
   The policy is now disabled.

Denial of service implications

The account lockout mechanism may be used to create a denial of service condition by repeatedly attempting to log in to an account using an incorrect password. Selected privileged accounts are exempted from the account lockout policy to prevent them from being locked out from a denial of service attack. However these privileged accounts may then become the target of password guessing attacks. Audit logs may be examined to monitor if such attacks are attempted.

Authentication model

This section discusses the authentication model of the switch management channel connections using the `aaaConfig` command. Fabric OS 6.x supports the use of both the local user database and the RADIUS service at the same time; and the local user database and LDAP using Microsoft’s Active Directory in Windows at the same time. Table 12 on page 66 outlines the available command options.

When configured to use RADIUS or LDAP, the switch acts as a network access server (NAS) and RADIUS or LDAP client. The switch sends all authentication, authorization, and accounting (AAA) service requests to the RADIUS or LDAP server. The RADIUS or LDAP server receives the request, validates the request, and sends its response back to the switch.

The supported management access channels that will integrate with RADIUS and LDAP include serial port, Telnet, SSH, Web Tools, and API. All these require the switch IP address or name to connect. The RADIUS server accepts both IPv4 and IP address formats, while LDAP server accepts only an IPv4 address.

A switch can be configured to try both RADIUS or LDAP and local switch authentication.

For systems such as the HP 4/256 SAN Director and DC SAN Backbone Director (DC Director), the switch IP addresses are aliases of the physical Ethernet interfaces on the CP blades. When specifying client IP addresses for the logical switches in such systems, make sure the CP IP addresses are used. For accessing both the active and standby CP, and for the purpose of HA failover, both CP IP addresses of a Director should be included in the RADIUS or LDAP server configuration.

When configured for RADIUS or LDAP, a switch becomes a RADIUS or LDAP client. In either of these configurations, authentication records are stored in the RADIUS or LDAP host server database. Login and logout account name, assigned role, and time-accounting records are also stored on the RADIUS or LDAP server for each user.

By default, the RADIUS and LDAP services are disabled, so AAA services default to the switch local database.

To enable RADIUS or LDAP service, it is strongly recommended that you access the CLI through an SSH connection so that the shared secret is protected. Multiple login sessions can configure simultaneously, and the last session to apply a change leaves its configuration in effect. After a configuration is applied, it persists after a reboot or an HA failover.

To enable LDAP service, you will need to install a certificate on the Microsoft Active Directory server.

The configuration applies to all switches and on a Director the configuration replicates itself on a standby CP blade if one is present. It is saved in a configuration upload and applied in a configuration download.

You should configure at least two RADIUS servers so that if one fails, the other will assume service.

You can set the configuration with both RADIUS or LDAP service and local authentication enabled so that if the RADIUS or LDAP servers do not respond due to power failure or network problems, the switch uses local authentication.
Consider the following effects of the use of RADIUS or LDAP service on other Fabric OS features:

- When RADIUS or LDAP service is enabled, all account passwords must be managed on the RADIUS or LDAP server. The Fabric OS mechanisms for changing switch passwords remain functional; however, such changes affect only the involved switches locally. They do not propagate to the RADIUS or LDAP server, nor do they affect any account on the RADIUS or LDAP server.

  When RADIUS or LDAP is set up for a fabric that contains a mix of switches with and without RADIUS or LDAP support, the way a switch authenticates users depends on whether or not a RADIUS or LDAP server is set up for that switch. For a switch with RADIUS or LDAP support and configuration, authentication bypasses the local password database. For a switch without RADIUS or LDAP support or configuration, authentication uses the switch’s local account names and passwords.

- The following behaviors apply to Web Tools:
  - Web Tools client and server keep a session open after a user is authenticated. A password change on a switch invalidates an open session and requires the user to log in again. When integrated with RADIUS or LDAP, a switch password change on the RADIUS or LDAP server does not invalidate an existing open session, although a password change on the local switch does.
  - If you cannot log in because of a RADIUS or LDAP server connection problem, Web Tools displays a message indicating server outage.

Table 12 lists authentication configuration options.

Table 12 Authentication configuration options

<table>
<thead>
<tr>
<th>aaaConfig options</th>
<th>Description</th>
<th>Equivalent setting in Fabric OS 5.1.0 and earlier</th>
</tr>
</thead>
<tbody>
<tr>
<td>--authspec &quot;local&quot;</td>
<td>Replaces --localonly. Default setting. Authenticates management connections against the local database only. If the password does not match or the user is not defined, the login fails.</td>
<td>Off On</td>
</tr>
<tr>
<td>--authspec &quot;radius&quot;</td>
<td>Replaces --radiusonly. Authenticates management connections against the RADIUS database(s) only. If the RADIUS service is not available or the credentials do not match, the login fails.</td>
<td>On Off</td>
</tr>
<tr>
<td>--authspec &quot;radius;local&quot;</td>
<td>Replaces --radiuslocal. Authenticates management connections against any RADIUS databases first. If RADIUS fails for any reason, authenticates against the local user database.</td>
<td>not supported not supported</td>
</tr>
<tr>
<td>--authspec &quot;radius;local&quot; --backup</td>
<td>Replaces --radiuslocalbackup. Authenticates management connections against any RADIUS databases. If RADIUS fails because the service is not available, authenticates against the local user database.</td>
<td>On On</td>
</tr>
</tbody>
</table>
To set the switch authentication mode:

1. Connect to the switch and log in using an admin account.
2. Enter this command:

    switch:admin> aaaConfig --authspec ["radius" | "ldap" | "radius;local" | "ldap;local" --backup]

Creating Fabric OS user accounts

RADIUS and LDAP servers allow you to set up user accounts by their true network-wide identity rather than by the account names created on a Fabric OS switch. With each account name, assign the appropriate switch access roles.

RADIUS and LDAP support all the defined RBAC roles described in Table 8 on page 54.

Users must enter their assigned RADIUS or LDAP account name and password when logging in to a switch that has been configured with RADIUS or LDAP. After the RADIUS or LDAP server authenticates a user, it responds with the assigned switch role in a Brocade Vendor-Specific Attribute (VSA). If the response does not have a VSA role assignment, the User role is assigned. If no Administrative Domain is assigned, then the user is assigned to the default Admin Domain AD0.

The syntax used for assigning VSA-based account switch roles on a RADIUS server is described in Table 13.

Table 13 Syntax for VSA-based account roles

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>26</td>
<td>1 octet</td>
</tr>
<tr>
<td>Length</td>
<td>7 or higher</td>
<td>1 octet, calculated by the server</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>1588</td>
<td>4 octet, Brocade’s SMI Private Enterprise Code</td>
</tr>
</tbody>
</table>
Managing Fabric OS users on the RADIUS server

All existing Fabric OS mechanisms for managing local switch user accounts and passwords remain functional when the switch is configured to use the remote authentication dial-in user service (RADIUS). Changes made to the local switch database do not propagate to the RADIUS server, nor do the changes affect any account on the RADIUS server.

Windows 2000 IAS

For example, to configure a Windows 2000 internet authentication service (IAS) server to use VSA to pass the Admin role to the switch in the dial-in profile, the configuration specifies the Vendor code (1588), Vendor-assigned attribute number (1), and attribute value (admin), as shown in the following:

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor type</td>
<td>1</td>
<td>1 octet, Brocade-Auth-Role; valid attributes for the Brocade-Auth-Role are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SwitchAdmin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ZoneAdmin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FabricAdmin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BasicSwitchAdmin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Admin</td>
</tr>
<tr>
<td>Optional</td>
<td>2</td>
<td>Specifies the Admin Domain member list. For more information, see “RADIUS configuration and Admin Domains” on page 69.</td>
</tr>
<tr>
<td>Brocade-AVPairs1</td>
<td></td>
<td>Brocade-AVPairs</td>
</tr>
<tr>
<td>3</td>
<td>Brocade-AVPairs2</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Brocade-AVPairs3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Brocade-AVPairs4</td>
<td></td>
</tr>
<tr>
<td>Optional</td>
<td>2 or higher</td>
<td>1 octet, calculated by server, including vendor-type and vendor-length</td>
</tr>
<tr>
<td>Attribute-specific data</td>
<td>ASCII string</td>
<td>Multiple octet, maximum 253, indicating the name of the assigned role and other supported attribute values such as Admin Domain member list.</td>
</tr>
</tbody>
</table>
Linux FreeRadius server

For the configuration on a Linux FreeRadius server, define the following in a vendor dictionary file called dictionary.brocade. Include the values outlined in Table 14.

Table 14  dictionary.brocade file entries

<table>
<thead>
<tr>
<th>Include</th>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VENDOR</td>
<td>Brocade</td>
<td>1588</td>
</tr>
<tr>
<td>ATTRIBUTE</td>
<td>Brocade-Auth-Role</td>
<td>string Brocade</td>
</tr>
<tr>
<td></td>
<td>AdminDomain</td>
<td></td>
</tr>
</tbody>
</table>

After you have completed the dictionary file, define the role for the user in a configuration file. For example, to grant the user jsmith the Admin role, you would add the following statement to the configuration file:

```plaintext
jsmith Auth-Type:= Local, User-Password == "jspassword"
Brocade-Auth-Role = "admin"
```

RADIUS configuration and Admin Domains

When configuring users with Admin Domains, you must also include the Admin Domain member list. This section describes the way that you configure attribute types for this configuration.

The values for the new attribute types use the syntax `key=val[:key=val]`, where `key` is a text description of attributes, `value` is the attribute value for the given key, the equal sign (`=`) is the separator between key and value, and the semi-colon (`;`) is an optional separator for multiple key-value pairs.

Multiple key-value pairs can appear for one Vendor-Type code. Key-value pairs with the same key name may be concatenated across multiple Vendor-Type codes. You can use any combination of the Vendor-Type codes to specify key-value pairs. Note that a switch always parses these attributes from Vendor-Type code 2 to Vendor-Type code 4.

Only two kinds of keys are accepted; all other keys are ignored. The following keys are accepted:

- **HomeAD** is the designated home Admin Domain for the account. The valid value is between 0 to 255, inclusive. The first valid HomeAD key-value pair is accepted by the switch, and any additional HomeAD key-value pairs are ignored.
- **ADList** is a comma-separated list of Administrative Domain numbers to which this account is a member. Valid numbers range from 0 to 255, inclusive. A dash between two numbers specifies a range. Multiple ADList key-value pairs within the same or across the different Vendor-Type codes are concatenated. Multiple occurrences of the same AD number are ignored.

RADIUS authentication requires that the account have a valid role through the attribute type `Brocade-Auth-Role`. The additional attribute values ADList and HomeAD are optional. If they are unspecified, the account can log in with AD0 as its member list and home Admin Domain. If there is an error in ADList or HomeAD specification, the account cannot log in until the AD list is corrected; an error message is displayed.

For example, on a Linux FreeRadius Server, the user (user-za) with the following settings takes the “ZoneAdmin” role, with AD member list: 1, 2, 4, 5, 6, 7, 8, 9, 12; the Home Admin Domain will be 1.

```plaintext
user-za Auth-Type := Local, User-Password == "password"
Brocade-Auth-Role = "ZoneAdmin",
Brocade-AVPairs1 = "ADList=1,2,6,
Brocade-AVPairs2 = "ADList=4-8;ADList=7,9,12"
```

In the next example, on a Linux FreeRadius Server, the user takes the “Operator” role, with ADList 1, 2, 4, 5, 6, 7, 8, 9, 12, 20 and homeAD 2.

```plaintext
user-opr Auth-Type := Local, User-Password == "password"
Brocade-Auth-Role = "operator",
Brocade-AVPairs1 = "ADList=1,2;HomeAD=2",
Brocade-AVPairs2 = "ADList=4-8,20;ADList=7,9,12"
```
Configuring the RADIUS server

You must know the switch IP address, in either IPv4 or IPv6 notation, or name to connect to switches. Use the ipAddrShow command to display a switch IP address.

For Directors (chassis-based systems), the switch IP addresses are aliases of the physical Ethernet interfaces on the CP blades. When specifying client IP addresses for the logical switches in such systems, make sure the CP blade IP addresses are used. For accessing both the active and standby CP blade, and for the purpose of HA failover, both of the CP blade IP addresses should be included in the RADIUS server configuration.

User accounts should be set up by their true network-wide identity, rather than by the account names created on a Fabric OS switch. Along with each account name, the administrator should assign appropriate switch access roles. To manage a fabric, these roles can be User, Admin, and SecurityAdmin.

When they log in to a switch configured with RADIUS, users enter their assigned RADIUS account names and passwords at the prompt. After the RADIUS server authenticates a user, it responds with the assigned switch role in a Brocade Vendor-Specific Attribute (VSA), as defined in the RFC. An Authentication-Accept response without such VSA role assignment automatically assigns the user role.

The following sections describe how to configure a RADIUS server to support clients under different operating systems.

Linux

The following procedures work for FreeRADIUS on Solaris and Red Hat Linux. FreeRADIUS is a freeware RADIUS server that you can find at the following website:

www.freeradius.org

Follow the installation instructions at the web site. FreeRADIUS runs on Linux (all versions), FreeBSD, NetBSD, and Solaris. If you make a change to any of the files used in this configuration, you must stop the server and restart it for the changes to take effect.

FreeRADIUS installation places the configuration files in $PREFIX/etc/raddb. By default, the PREFIX is /usr/local.

Configuring RADIUS service on Linux consists of the following tasks:

- Adding the Brocade attribute to the server
- Creating the user
- Enabling clients

To add the Brocade attribute to the server:

1. Create and save the file $PREFIX/etc/raddb/dictionary.brocade with the following information:

```
# # Brocade FabricOS 5.0.1 dictionary
#
VENDOR Brocade 1588
#
attribute 1 defined to be Brocade-Auth-Role
# string defined in user configuration
#
ATTRIBUTE Brocade-Auth-Role 1 string Brocade
```

This defines the Brocade vendor ID as 1588, the Brocade attribute 1 as Brocade-Auth-Role, and it is a string value.

2. Open the file $PREFIX/etc/raddb/dictionary in a text editor and add the line:

$INCLUDE dictionary.brocade

As a result, the file dictionary.brocade is located in the RADIUS configuration directory and loaded for use by the RADIUS server.
To create the user:

- Open the $PREFIX/etc/raddb/user file in a text editor and add user names and roles for users who will be accessing the switch and authenticating RADIUS.

  The user will log in using the role specified with Brocade-Auth-Role. The valid roles include Root, Admin, SwitchAdmin, ZoneAdmin, SecurityAdmin, BasicSwitchAdmin, FabricAdmin, Operator and User. You must use quotation marks around “password” and “role”.

  For example, to set up an account called JohnDoe with the Admin role:

  JohnDoe Auth-Type := Local, User-Password == "johnPassword" Brocade-Auth-Role = "admin"

  The next example uses the local system password file to authenticate users.

  JohnDoe Auth-Type := System, Brocade-Auth-Role = "admin"

  When you use Network Information Service (NIS) for authentication, the only way to enable authentication with the password file is to force the switch to authenticate using Password Authentication Protocol (PAP); this requires the -a pap option with the aaaConfig command.

Clients are the switches that will use the RADIUS server; each client must be defined. By default, all IP addresses are blocked.

4/256 SAN Director and DC SAN Backbone Director (short name, DC Director) models send their RADIUS requests using the IP address of the active CP. When adding clients, add both the active and standby CP IP addresses so that, in the event of a failover, users can still log in to the switch.

To enable clients:

1. Open the $PREFIX/etc/raddb/client.config file in a text editor and add the switches that are to be configured as RADIUS clients.

   For example, to configure the switch at IP address 10.32.170.59 as a client:

   client 10.32.170.59
   secret    = Secret
   shortname = Testing Switch
   nastype   = other

   In this example, shortname is an alias used to easily identify the client. Secret is the shared secret between the client and server. Make sure the shared secret matches that configured on the switch (see “To add a RADIUS server to the switch configuration:” on page 76).

   Save the file $PREFIX/etc/raddb/client.config then start the RADIUS server as follows:

   $PREFIX/sbin/radiusd

Windows 2000

The instructions for setting up RADIUS on a Windows 2000 server are listed here for your convenience but are not guaranteed to be accurate for your network environment. Always check with your system administrator before proceeding with setup.

Configuring RADIUS service on Windows 2000 consists of the following tasks:

- Installing internet authentication service (IAS)
  For more information and instructions on installing IAS, refer to the Microsoft web site.

- Enabling the Challenge Handshake Authentication Protocol (CHAP)
  If CHAP authentication is required, then Windows must be configured to store passwords with reversible encryption. Reverse password encryption is not the default behavior; it must be enabled.

  If a user is configured prior to enabling reverse password encryption, then the user’s password is stored and cannot utilize CHAP. To use CHAP, the password must be re-entered after encryption is enabled. If the password is not re-entered, then CHAP authentication will not work and the user will be unable to authenticate from the switch.

- Configuring a user
  IAS is the Microsoft implementation of a RADIUS server and proxy. IAS uses the Windows native user database to verify user login credentials; it does not list specific users, but instead lists user groups.
Each user group should be associated with a specific switch login role. For example, you should configure a user group for root, admin, factory, switchadmin, and user, and then add any users whose logins you want to associate to the appropriate group.

- Configuring the server

To enable CHAP:

1. From the Windows Start menu, select Programs > Administrative Tools > Local Security Policy to open the Local Security Settings window.
2. In the Local Security Settings window, expand the Account Policies folder and select the Password Policy folder.
3. From the list of policies in the Password Policy folder, right-click Store password using reversible encryption for all users in the domain, and select Security from the pop-up menu.
4. An additional Local Security Settings window appears. Click the Enabled radio button and then click OK.

To configure users:

1. From the Windows Start menu, select Programs > Administrative Tools > Computer Management to open the Computer Management window.
2. In the Computer Management window, expand the Local Users and Groups folder and select the Groups folder.
3. Right-click the Groups folder and select New Group from the pop-up menu.
4. In the New Group window, provide a Name and Description for the group and click Add.
5. In the Select Users or Groups window, select the user (who should already have been configured) you want to add to the group and click Add.
6. Repeat this for every user you want to add. When you have completed adding all users, click OK.
7. In the New Group window, verify the users you added in step 4 appear in the Members field; then click Create to create this group.
   
   The new groups are created for each login type (admin, switchAdmin, user).

To configure the RADIUS server:

1. From the Windows Start menu, select Programs > Administrative Tools > Internet Authentication Service to open the Internet Authentication Service window.
2. In the Internet Authentication Service window, right-click the Clients folder and select New Client from the pop-up menu.
   
   A client is the device that uses the RADIUS server; in this case, it is the switch.
3. In the Add Client window, provide the following:
   
   Friendly name—The friendly name should be an alias that is easily recognizable as the switch to which you are connecting.
   
   Protocol—Select RADIUS as the protocol.
4. In the Add RADIUS Client window, provide the following:
   
   Client address (IP or DNS)—Enter the IP address of the switch.
   
   Client-Vendor—Select RADIUS Standard.
   
   Shared secret—Provide a password. Shared secret is a password used between the client device and server to prevent IP address spoofing by unwanted clients. Keep your shared secret password in a safe place. You will need to enter this password in the switch configuration.

After clicking Finish, repeat step 2 through step 4 for all switches on which RADIUS authentication will be used.

5. In the Internet Authentication Service window, right-click the Remote Access Policies folder; then select New Remote Access Policy from the pop-up window.
   
   A remote access policy must be created for each login role (Root, Admin, Factory, SwitchAdmin, and User) for which you want to use RADIUS. Apply this policy to the user groups that you already created.
6. In the Add Remote Access Policy window, enter an easily identifiable **Policy friendly name** that will enable you to see the switch login for which the policy is being created; then click **Next**.

7. After the Add Remote Access Policy window refreshes, click **Add**.

8. In the Select Attribute window, select **Windows Groups** and click **Add**.

9. In the Groups window, click **Add**.

10. In the Select Groups window, select the user-defined group for which you are creating a policy and click **Add**. After adding all appropriate groups, click **OK**. In the Groups window, click **OK**.

11. In the Add Remote Access Policy window, confirm that the Conditions section displays the group(s) that you selected and click **Next**.

12. After the Add Remote Access Policy window refreshes, select the **Grant remote access permission** radio button and click **Next**.

13. After the Add Remote Access Policy window refreshes again, click **Edit Profile**.

14. In the Edit Dial-in Profile window, click the **Authentication** tab and check only the **Encrypted Authentication (CHAP)** and **Unencrypted Authentication (PAP, SPAP)** checkboxes; then click the **Advanced** tab and click **Add**.

15. In the Add Attributes window, select **Vendor-Specific** and click **Add**.

16. In the Multivalued Attribute Information window, click **Add**.

17. In the Vendor-Specific Attribute Information window, click the **Enter Vendor Code** radio button and enter the value **1588**. Click the **Yes. It conforms** radio button, and then click **Configure Attribute...**

18. In the Configure VSA (RFC compliant) window, enter the following values and click **OK**.
   
   **Vendor-assigned attribute number**—Enter the value **1**.
   
   **Attribute format**—Enter **String**.
   
   **Attribute value**—Enter the login role (Root, Admin, SwitchAdmin, User, etc.) the user group must use to log in to the switch.

19. In the Multivalued Attribute Information window, click **OK**.

20. In the Edit Dial-in Profile window, remove all additional parameters (except the one you just added, “Vendor-Specific”) and click **OK**.

21. In the Add Remote Access Policy window, click **Finish**.

After returning to the Internet Authentication Service window, repeat step 5 through step 21 to add additional policies for all login types for which you want to use the RADIUS server. After this is done, you can configure the switch.

**LDAP configuration and Microsoft’s Active Directory**

LDAP provides user authentication and authorization using Microsoft’s Active Directory service in conjunction with LDAP on the switch. The following are restrictions when using LDAP:

- In Fabric OS 6.x there will be no password change through Active Directory.
- There is no automatic migration of newly created users from local switch database to Active Directory. This is a manual process explained later.
- LDAP authentication is used on the local switch only and not for the entire fabric.

Roles for users can be added through the Microsoft Management Console. Groups created in Active Directory must correspond directly to the RBAC user roles on the switch. Role assignments can be achieved by including the user in the respective group. A user can be assigned to multiple groups like Switch Admin and Security Admin. For more information on RBAC roles, see “Using Role-Based Access Control (RBAC)” on page 54.

**NOTE:** All instructions involving Microsoft’s Active Directory can be obtained from [www.microsoft.com](http://www.microsoft.com). Confer with your network administrator prior to configuration for any special needs your network environment may have.
To set up LDAP:

1. Install a certificate on the Windows Active Directory server for LDAP. Create a user in Microsoft Active Directory server. For instructions on how to create a user, refer to www.microsoft.com or Microsoft documentation to create a user in your Active Directory.

2. Create a group name that uses the switch’s role name so that the Active Directory group’s name is the same as the switch’s role name.

3. Associate the user to the group by adding the user to the group. For instructions on how to create a user refer to www.microsoft.com or Microsoft documentation to create a user in your Active Directory.

4. Add the user’s Administrative Domains to the CN_list by editing the adminDescription value.

   This will map the admin domains to the user name. Multiple admin domains can be added as a string value separated by the underscore character (_).

To create a user:

To create a user in Active Directory, refer to www.microsoft.com or Microsoft documentation. There are no special attributes.

To create a group:

To create a group in Active Directory, refer to www.microsoft.com or Microsoft documentation. You will need to verify that the group uses the following attributes:

• The name of the group has to match the RBAC role.
• The Group Type must be Security.
• The Group Scope must be Global.

To assign the group (role) to the user:

To assign the user to a group in the Active Directory, refer to www.microsoft.com or Microsoft documentation. You will need to verify that the user has the following attributes:

1. Update the memberOf field with the login role (Root, Admin, SwitchAdmin, User, etc.) that the user must use to log in to the switch.

2. From the Windows Start menu, select Programs> Administrative Tools> ADSI.msc

   ADSI is a Microsoft Windows Resource Utility. This will need to be installed to proceed with the rest of the setup. For Windows 2003, this utility comes with Service Pack 1 or you can download this utility from the Microsoft website.

3. Go to CN=Users0

4. Right click on select Properties. Click the Attribute Editor tab.

5. Double-click the adminDescription attribute.

   This opens the String Attribute Editor dialog box.

6. Enter the value for the admin domains separated by an underscore (_ ) into the Value field.

   Example
   
   adlist_0_10_200_endAd
   Home Admin Domain (homeAD) for the user will be the first value in the adlist (Admin Domain list). If a user has no values assigned in the adlist attribute, then the homeAD ‘0’ will be the default administrative domain for the user.

   NOTE: You can perform batch operations using the Ldifde.exe utility. For more information on importing and exporting schemas, refer to your Microsoft documentation or visit www.microsoft.com.
Configuring authentication servers on the switch

RADIUS and LDAP configuration of the switch is controlled by the `aaaConfig` command.

At least one RADIUS or LDAP server must be configured before you can enable RADIUS or LDAP service. You can configure the RADIUS or LDAP service even if it is disabled on the switch. You can configure up to five RADIUS or LDAP servers. You must be logged in as admin or switchadmin to configure the RADIUS service.

**NOTE:** On dual-CP switches (the 4/256 SAN Director and the DC Director), the switch sends its RADIUS or LDAP request using the IP address of the active CP. When adding clients, add both the active and standby CP IP addresses so that users can still log in to the switch in the event of a failover.

RADIUS or LDAP configuration is chassis-based configuration data. On platforms containing multiple switch instances, the configuration applies to all instances. The configuration is persistent across reboot and `firmwareDownload`. On a chassis-based system, the command must replicate the configuration to the standby CP.

Multiple login sessions can invoke the command simultaneously. The last session that applies the change will be the one whose configuration is in effect. This configuration is persistent after an HA failover.

The RADIUS or LDAP servers are contacted in the order they are listed, starting from the top of the list and moving to the bottom.

The following procedures show how to use the `aaaConfig` command to set up a switch for RADIUS or LDAP service.

To display the current RADIUS configuration:

1. Connect to the switch and log in using an admin account.
2. Enter this command:
   ```bash
   switch:admin> aaaConfig --show
   ```
   If a configuration exists, its parameters are displayed. If RADIUS or LDAP service is not configured, only the parameter heading line is displayed. Parameters include:

   - **Position**: The order in which servers are contacted to provide service.
   - **Server**: The server names or IPv4 or IPv6 addresses.
   - **Port**: The server ports.
   - **Secret**: The shared secrets.
   - **Timeouts**: The length of time servers have to respond before the next server is contacted.
   - **Authentication**: The type of authentication being used on servers.
To add a RADIUS server to the switch configuration:
1. Connect to the switch and log in using an admin account.
2. Enter this command:
   ```
   switch:admin> aaaConfig --add <server> [-p port] [-s secret] [-t timeout] [-a pap | chap | peap-mschapv2]
   ```
   - **server**: Enter either a server name or IPv4 or IPv6 address. Avoid duplicating server listings (that is, listing the same server once by name and again by IP address). Up to five servers can be added to the configuration.
   - **-p port**: Optional: Enter a server port. The default is port 1812.
   - **-s secret**: Optional: Enter a shared secret. The default is "sharedsecret". Secrets can be from 8 to 40 alphanumeric characters long. Make sure that the secret matches that configured on the server.
   - **-t timeout**: Optional: Enter the length of time (in seconds) that the server has to respond before the next server is contacted. The default is three seconds. Time-out values can range from 1 to 30 seconds.
   - **-a [pap|chap|peap-mschapv2]**: Specify PAP, CHAP or PEAP as authentication protocol. Use peap-mschapv2 to provide encrypted authentication channel between the switch and server.

To add an LDAP server to the switch configuration:
1. Connect to the switch and log in using an admin account.
2. Enter this command:
   ```
   switch:admin> aaaConfig --add <server> [-p port] [-t timeout] [-d domain_name]
   ```
   - **server**: Enter either a server name or IPv4 address. Microsoft’s Active Directory does not support IPv6 addresses. Avoid duplicating server listings (that is, listing the same server once by name and again by IP address). Up to five servers can be added to the configuration.
   - **-p port**: Optional: Enter a server port. The default is port 389.
   - **-t timeout**: Optional: Enter the length of time (in seconds) that the server has to respond before the next server is contacted. The default is three seconds. Time-out values can range from 1 to 30 seconds.
   - **-d domain_name**: Enter the name of the Windows domain.

At least one RADIUS or LDAP server must be configured before you can enable the RADIUS or LDAP service.

If no RADIUS or LDAP configuration exists, turning it on triggers an error message. When the command succeeds, the event log indicates that the configuration is enabled or disabled.
NOTE: When the RADIUS authentication mode is set to radius;local, you cannot downgrade the Fabric OS to any version earlier than 5.2.0. Previous versions do not support the radius;local mode.

When the LDAP authentication mode is set to ldap;local, you cannot downgrade the Fabric OS to any version earlier than 6.x. Previous versions do not support the ldap;local mode.

To enable and disable a RADIUS or LDAP server:
1. Connect to the switch and log in using an admin account.
2. Enter this command to enable RADIUS or LDAP using the local database:
   ```bash
   switch:admin> aaaconfig --authspec "<radius | ldap>;local"
   ```
   where you specify the type of server as either RADIUS or LDAP, but not both. Local is used for local authentication if the user authentication fails on the RADIUS or LDAP server.
   Example
   ```bash
   switch:admin> aaaconfig --authspec "radius;local" --backup
   ```

To delete a RADIUS or LDAP server from the configuration:
1. Connect to the switch and log in using an admin account.
2. Enter this command:
   ```bash
   switch:admin> aaaConfig --remove server | all
   ```
   Enter either the name or IP address of the server to be removed.

When the command succeeds, the event log indicates that the server is removed.

To change a RADIUS server configuration
1. Connect to the switch and log in using an admin account.
2. Enter this command:
   ```bash
   switch:admin> aaaConfig --change server [-p port] [-s shared secret] [-t timeout]
   [-a pap|chap|peap-mschapv2]
   ```
   server Enter either the name or IP address of the server to be changed.
   -p port Optional: Enter a server port. The default is 1812.
   -s shared secret Optional: Enter a shared secret.
   -t timeout Optional: Enter the length of time (in seconds) the server has to respond before the next server is contacted.
   -a [pap|chap|peap-mschapv2] Specify PAP, CHAP or PEAP as authentication protocol. Use peap-mschapv2 to provide security on the switch.

NOTE: Protected Extensible Authentication Protocol (PEAP) is used to authenticate users and clients. It is based on extensible authentication protocol (EAP) and transport layer security (TLS).

When PEAP is configured on the switch, clients running Fabric Manager cannot authenticate.
To change an LDAP server configuration:
1. Connect to the switch and log in using an admin account.
2. Enter this command:

```bash
switch:admin> aaaConfig --change server [-p port] [-t timeout] [-d domain_name]
```

- **server**: Enter either a server name or IPv4 address. Microsoft’s Active Directory does not support IPv6 addresses. Avoid duplicating server listings (that is, listing the same server once by name and again by IP address). Up to five servers can be added to the configuration.
- **-p port**: Optional: Enter a server port. The default is port 389.
- **-t timeout**: Optional: Enter the length of time (in seconds) that the server has to respond before the next server is contacted. The default is three seconds. Time-out values can range from 1 to 30 seconds.
- **-d domain_name**: Enter the name of the Windows domain.

To change the order in which RADIUS or LDAP servers are contacted for service:
1. Connect to the switch and log in using an admin account.
2. Enter this command:

```bash
switch:admin> aaaConfig --move server to_position
```

- **server**: Enter either the name or IP address of the server whose position is to be changed.
- **to_position**: Enter the position number to which the server is to be moved.

When the command succeeds, the event log indicates that a server configuration is changed.

### Enabling and disabling local authentication as backup

It is useful to enable local authentication so that the switch can take over authentication locally if the RADIUS or LDAP servers fail to respond because of power outage or network problems. To enable or disable local authentication, enter the following command for RADIUS:

```bash
switch:admin> aaaconfig --authspec "radius;local" --backup
```

or for LDAP,

```bash
switch:admin> aaaconfig --authspec "ldap;local" --backup
```

For details about this command see Table 12 on page 66.

When local authentication is enabled and the RADIUS or LDAP servers fail to respond, you can log in to the default switch accounts (admin and user) or any user-defined account. You must know the passwords of these accounts.

When the command succeeds, the event log indicates that local database authentication is disabled or enabled.

### Boot PROM password

The boot PROM password provides an additional layer of security by protecting the boot PROM from unauthorized use. Setting a recovery string for the boot PROM password enables you to recover a lost boot PROM password by contacting HP. Without the recovery string, a lost boot PROM password cannot be recovered.

You should set the boot PROM password and the recovery string on all switches, as described in “Setting the boot PROM password with a recovery string” on page 79. If your site procedures dictate that you set the boot PROM password without the recovery string, see “Setting the boot PROM password without a recovery string” on page 81.
Setting the boot PROM password with a recovery string

To set the boot PROM password with a recovery string, refer to the section that applies to your switch model.

**NOTE:** Setting the boot PROM password requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted. You should perform this procedure during a planned down time.


The instructions contained within this section are only for the switches listed in the title. If your switch is not listed, please contact HP for instructions.

To set the boot PROM password for a switch with a recovery string:

1. Connect to the serial port interface.
2. Press **ESC** within four seconds after the message “Press escape within 4 seconds...” displays.
   
   The following options are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start system. Continues the system boot process.</td>
</tr>
<tr>
<td>2</td>
<td>Recovery password. Lets you set the recovery string and the boot PROM password.</td>
</tr>
<tr>
<td>3</td>
<td>Enter command shell. Provides access to boot parameters.</td>
</tr>
</tbody>
</table>

3. Enter 2.
   
   If no password was previously set, the following message displays:

   Recovery password is NOT set. Please set it now.

   If a password was previously set, the following messages display:

   Send the following string to Customer Support for password recovery:
   
   afHTpyLsDo1Pz0Pk5GzhIw==

   Enter the supplied recovery password.

   Recovery Password:

4. Enter the recovery password (string).
   
   The recovery string must be between 8 and 40 alphanumeric characters. A random string that is 15 characters or longer is recommended for higher security. The firmware prompts for this password only once. It is not necessary to remember the recovery string because it is displayed the next time you enter the command shell.

   The following prompt displays:

   New password:

5. Enter the boot PROM password, then re-enter it when prompted. The password must be eight alphanumeric characters (any additional characters are not recorded). Record this password for future use.

   The new password is automatically saved.

6. Type **reset** at the prompt to reboot the switch.
The boot PROM and recovery passwords must be set for each CP blade on the 4/256 SAN Director or DC Director.

To set the boot PROM password for a Director with a recovery string:

1. Connect to the serial port interface on the standby CP blade.
2. Connect to the active CP blade by serial or Telnet and enter the `haDisable` command to prevent failover during the remaining steps.
3. Reboot the standby CP blade by sliding the On/Off switch on the ejector handle of the standby CP blade to Off, and then back to On.
4. Press ESC within four seconds after the message “Press escape within 4 seconds...” displays.

The following options are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start system. Continues the system boot process.</td>
</tr>
<tr>
<td>2</td>
<td>Recovery password. Lets you set the recovery string and the boot PROM password.</td>
</tr>
<tr>
<td>3</td>
<td>Enter command shell. Provides access to boot parameters.</td>
</tr>
</tbody>
</table>

5. Enter 2.

   If no password was previously set, the following message displays:
   ```
   Recovery password is NOT set. Please set it now.
   ```
   
   If a password was previously set, the following messages display:
   ```
   Send the following string to Customer Support for password recovery:
   afHTpyLsDo1Pz0Pk5GzhIw==
   Enter the supplied recovery password.
   Recovery Password:
   ```

6. Enter the recovery password (string).

   The recovery string must be between 8 and 40 alphanumeric characters. A random string that is 15 characters or longer is recommended for higher security. The firmware only prompts for this password once. It is not necessary to remember the recovery string because it is displayed the next time you enter the command shell.

   The following prompt displays:
   ```
   New password:
   ```

7. Enter the boot PROM password, then re-enter it when prompted. The password must be eight alphanumeric characters (any additional characters are not recorded). Record this password for future use.

   The new password is automatically saved (the `saveEnv` command is not required).

8. Connect to the active CP blade using serial or Telnet and enter the `haEnable` command to restore High Availability; then fail over the active CP blade by entering the `haFailover` command.

9. Connect the serial cable to the serial port on the new standby CP blade (previously the active CP blade).

10. Repeat step 2 through step 7 for the new standby CP blade (each CP blade has a separate boot PROM password).

11. Connect to the active CP blade by serial or Telnet and enter the `haEnable` command to restore High Availability.
Setting the boot PROM password without a recovery string

Although you can set the boot PROM password without also setting the recovery string, it is strongly recommended that you set both the password and the string as described in “Setting the boot PROM password with a recovery string” on page 79. If your site procedures dictate that you must set the boot PROM password without the string, follow the procedure that applies to your switch model.

Setting the boot PROM password requires accessing the boot prompt, which stops traffic flow through the switch until the switch is rebooted. You should perform this procedure during a planned down time.


The password recovery instructions contained within this section are only for the switches listed in the title. If your switch is not listed, contact HP for instructions.

To set the boot PROM password for a switch without a recovery string:

1. Create a serial connection to the switch.
2. Enter the `reboot` command to reset the switch.
3. Press **ESC** within four seconds after the message “Press escape within 4 seconds...” displays.
   - The following options are available:
     - **Option** | **Description**
       - 1  | Start system. Continues the system boot process.
       - 2  | Recovery password. Lets you set the recovery string and the boot PROM password.
       - 3  | Enter command shell. Provides access to boot parameters.
4. Enter 3.
5. At the shell prompt, enter the `passwd` command.

**NOTE:** The `passwd` command only applies to the boot PROM password when it is entered from the boot interface.

6. Enter your boot PROM password at the prompt, then re-enter it when prompted. The password must be eight alphanumeric characters (any additional characters are not recorded). Record this password for future use.
7. Enter the `saveEnv` command to save the new password.
8. Enter the `reboot` command to reset the switch.

**4/256 SAN Director and DC SAN Backbone Director (short name, DC Director)**

On 4/256 SAN Director and DC Director models, set the password on the standby CP blade, fail over, and then set the password on the previously active (now standby) CP blade to minimize disruption to the fabric.

To set the boot PROM password for a Director without a recovery string:

1. Determine the active CP blade by opening a Telnet session to either CP blade, connecting as admin, and entering the `haShow` command.
2. Connect to the active CP blade by serial or Telnet and enter the `haDisable` command to prevent failover during the remaining steps.
3. Create a serial connection to the standby CP blade.
4. Reboot the standby CP blade by sliding the On/Off switch on the ejector handle of the standby CP blade to Off, and then back to On. This causes the blade to reset.
5. Press **ESC** within four seconds after the message “Press escape within 4 seconds...” displays.
The following options are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start system.</td>
</tr>
<tr>
<td>2</td>
<td>Recovery password.</td>
</tr>
<tr>
<td>3</td>
<td>Enter command shell.</td>
</tr>
</tbody>
</table>

6. Enter **3**.
7. Enter the `passwd` command at the shell prompt.

**NOTE:** The `passwd` command only applies to the boot PROM password when it is entered from the boot interface.

8. Enter your boot PROM password at the prompt, then re-enter it when prompted. The password must be eight alphanumeric characters (any additional characters are not recorded). Record this password for future use.
9. Enter the `saveEnv` command to save the new password.
10. Reboot the standby CP blade by entering the `reset` command.
11. Connect to the active CP blade by serial or Telnet and enter the `haEnable` command to restore High Availability; then fail over the active CP blade by entering the `haFailover` command. Traffic resumes flowing through the newly active CP blade after it has completed rebooting.
12. Connect the serial cable to the serial port on the new standby CP blade (previously the active CP blade).
13. Repeat step 3 through step 10 for the new standby CP blade.
14. Connect to the active CP blade by serial or Telnet and enter the `haEnable` command to restore High Availability.

**Recovering forgotten passwords**

If you know the root password, you can use this procedure to recover the password for the default accounts of user, admin, and factory.

To recover passwords:

1. Open a CLI connection (serial or Telnet) to the switch.
   - OR
     - Connect to the primary FCS switch, if one exists in your fabric.
2. Log in as root.
3. Enter the command for the type of password that was lost:
   ```
   passwd user
   passwd admin
   passwd factory
   ```
4. Enter the requested information at the prompts.

To recover a lost root password or boot PROM password, contact HP. You must have previously set a recovery string to recover the boot PROM password.

**NOTE:** Contact HP to recover a lost root password or boot PROM password. You must have previously set a recovery string to recover the boot PROM password.
3 Configuring standard security features

This chapter provides information and procedures for configuring standard Fabric OS security features such as protocol and certificate management.

**IMPORTANT:** Secure Fabric OS is no longer supported in Fabric OS 6.x.

Secure protocols

Fabric OS supports the secure protocols shown in Table 15.

**Table 15** Secure protocol support

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Supports SSLv3, 128-bit encryption by default. Fabric OS uses SSL to support HTTPS. A certificate must be generated and installed on each switch to enable SSL.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Web Tools supports the use of HTTPS.</td>
</tr>
<tr>
<td>Secure File Copy (scp)</td>
<td>Configuration upload and download support the use of scp.</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>SNMPv1 and v2 are also supported.</td>
</tr>
</tbody>
</table>

Simple Network Management Protocol (SNMP) is a standard method for monitoring and managing network devices. Using SNMP components, you can program tools to view, browse, and manipulate switch variables and set up enterprise-level management processes.

Every switch carries an SNMP agent and Management Information Base (MIB). The agent accesses MIB information about a device and makes it available to a network manager station. You can manipulate information of your choice by trapping MIB elements using the Fabric OS CLI, Web Tools, or Fabric Manager.

The SNMP Access Control List (ACL) provides a way for the administrator to restrict SNMP get and set operations to certain hosts and IP addresses. This is used for enhanced management security in the storage area network.

For details on Brocade MIB files, naming conventions, loading instructions, and information about using Brocade’s SNMP agent, see the Fabric OS MIB Reference.

**Table 16** describes additional software or certificates that you must obtain to deploy secure protocols.

**Table 16** Items needed to deploy secure protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Host side</th>
<th>Switch side</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>SSH client</td>
<td>None</td>
</tr>
<tr>
<td>HTTPS</td>
<td>No requirement on host side except a browser that supports HTTPS</td>
<td>Switch IP certificate for SSL</td>
</tr>
<tr>
<td>Secure File Copy (scp)</td>
<td>SSH daemon, scp server</td>
<td>None</td>
</tr>
<tr>
<td>SNMPv1, SNMPv2, SNMPv3</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>
The security protocols are designed with the four main usage cases described in Table 17.

<table>
<thead>
<tr>
<th>Fabric</th>
<th>Management interfaces</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nonsecure</td>
<td>Nonsecure</td>
<td>No special setup is needed to use Telnet or HTTP.</td>
</tr>
<tr>
<td>Nonsecure</td>
<td>Secure</td>
<td>Secure protocols may be used. An SSL switch certificate must be installed if HTTPS is used.</td>
</tr>
<tr>
<td>Secure</td>
<td>Secure</td>
<td>Secure protocols are supported on Fabric OS v4.1.0 and later switches. Switches running earlier Fabric OS versions can be part of the secure fabric, but they do not support secure management. Secure management protocols must be configured for each participating switch. Nonsecure protocols may be disabled on non-participating switches. If SSL is used, then certificates must be installed.</td>
</tr>
<tr>
<td>Secure</td>
<td>Nonsecure</td>
<td>You must use SSH because Telnet is not allowed with some features, such as RADIUS. Nonsecure management protocols are necessary under these circumstances: The fabric contains switches running Fabric OS v3.2.0. The presence of software tools that do not support secure protocols: for example, Fabric Manager v4.0.0. The fabric contains switches running Fabric OS versions earlier than v4.4.0. Nonsecure management is enabled by default.</td>
</tr>
</tbody>
</table>

### Ensuring network security

To ensure security, Fabric OS supports secure shell (SSH) encrypted sessions in 4.1.x and later. SSH encrypts all messages, including the client’s transmission of password during login. The SSH package contains a daemon (sshd), which runs on the switch. The daemon supports a wide variety of encryption algorithms, such as Blowfish-CBC and AES.

**NOTE:** To maintain a secure network, you should avoid using Telnet or any other unprotected application when you are working on the switch.

The FTP protocol is also not secure. When you use FTP to copy files to or from the switch, the contents are in clear text. This includes the remote FTP server’s login and password. This limitation affects the following commands: `saveCore`, `configUpload`, `configDownload`, and `firmwareDownload`.

Commands that require a secure login channel must originate from an SSH session. If you start an SSH session, and then use the login command to start a nested SSH session, commands that require a secure channel will be rejected.

Fabric OS 4.1.0 and later supports SSH protocol version 2.0 (ssh2). For more information on SSH, refer to the SSH IETF website:

http://www.ietf.org/ids.by.wg/secsh.html

Configuring the Telnet protocol

Telnet is enabled by default. To prevent users from passing clear text passwords over the network when they connect to the switch, you can block the Telnet protocol using an IP Filter policy.

NOTE: Before blocking Telnet, make sure you have an alternate method of establishing a connection with the switch.

Blocking Telnet

To block Telnet:
1. Connect to the switch and log in as admin.
   Connect through some means other than Telnet: for example, through SSH.
2. Create a policy:
   
   ```
   ipfilter --create <policyname> -type < ipv4 | ipv6 >
   ```
   
   where `<policyname>` is the name of the new policy and `-type` specifies an IPv4 or IPv6 address.

   **Example**
   
   ```
   ipfilter --create block_telnet_v4 --type ipv4
   ```

   3. Add a rule to the policy, by typing the following command:
   
   ```
   ipfilter --addrule <policyname> -rule <rule_number> -sip <source_IP> -dp <dest_port> -proto <protocol> -act <deny>
   ```
   
   where `-sip` option can be given as any, `-dp` is the port number for telnet (23), and `-proto` is tcp.

   **Example**
   
   ```
   ipfilter --addrule block_telnet_v4 -rule 2 -sip any -dp 23 -proto tcp -act deny
   ```

   4. Save the new ipfilter policy by typing the following command:
   
   ```
   ipfilter --save [policyname]
   ```

   where `[policyname]` is the name of the policy and is optional.

   **Example**
   
   ```
   ipfilter --save block_telnet_v4
   ```

   5. Activate the new ipfilter policy by typing the following command:
   
   ```
   ipfilter --activate <policyname>
   ```

   where `<policyname>` is the name of the policy you created in step

   **Example**
   
   ```
   ipfilter --activate block_telnet_v4
   ```

Unblocking Telnet

To unblock Telnet:
1. Connect to the switch through a means other than Telnet (for example, SSH) and log in as admin.
2. Type in the following command:
   
   ```
   ipfilter -delete <telnet_policyname>
   ```

   where `<telnet_policyname>` is the name of the Telnet policy.

3. To permanently delete the policy, type the following command:
   
   ```
   ipfilter --save
   ```

   For more information on IP Filter policies, refer to “Configuring advanced security features” on page 99.
Blocking listeners

HP switches block Linux subsystem listener applications that are not used to implement supported features and capabilities. Table 18 lists the listener applications that Brocade switches either block or do not start.

<table>
<thead>
<tr>
<th>Listener application</th>
<th>4/256 SAN Director and DC SAN Backbone Director (short name, DC Director)</th>
<th>HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP c-Class BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router FC10-6, FC4-48, FC4-16IP, FC8-16, FC8-32, FC8-48, and FR4-18i blades</th>
</tr>
</thead>
<tbody>
<tr>
<td>chargen</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>echo</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>daytime</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>discard</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>ftp</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>rexec</td>
<td>Block with packet filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>rsh</td>
<td>Block with packet filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>rlogin</td>
<td>Block with packet filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>time</td>
<td>Block with packet filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>rstats</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>rusers</td>
<td>Disabled</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Accessing switches and fabrics

If you are using the FC-FC Routing Service, be aware that the secModeEnable command is no longer supported in Fabric OS 6.x.

Table 19 lists the defaults for accessing hosts, devices, switches, and zones.

<table>
<thead>
<tr>
<th>Access default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>Any host can access the fabric by SNMP</td>
</tr>
<tr>
<td></td>
<td>Any host can Telnet to any switch in the fabric</td>
</tr>
<tr>
<td></td>
<td>Any host can establish an HTTP connection to any switch in the fabric</td>
</tr>
<tr>
<td></td>
<td>Any host can establish an API connection to any switch in the fabric</td>
</tr>
<tr>
<td>Devices</td>
<td>All devices can access the Management Server</td>
</tr>
<tr>
<td></td>
<td>Any device can connect to any FC port in the fabric</td>
</tr>
<tr>
<td>Switch access</td>
<td>Any switch can join the fabric</td>
</tr>
<tr>
<td></td>
<td>All switches in the fabric can be accessed through a serial port</td>
</tr>
<tr>
<td>Zoning</td>
<td>No zoning is enabled</td>
</tr>
</tbody>
</table>
Port configuration

The following Table provides information on ports that the switch uses. When configuring the switch for various policies, take into consideration firewalls and other devices that may sit between switches in the fabric and your network or between the managers and the switch.

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Common use</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>SSH</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>TCP</td>
<td>Telnet</td>
<td>Use the <code>ipfilter</code> command to block the port.</td>
</tr>
<tr>
<td>123</td>
<td>TCP</td>
<td>NTP</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>HTTP</td>
<td>Use the <code>ipfilter</code> command to block the port.</td>
</tr>
<tr>
<td>111</td>
<td>TCP</td>
<td>sunrpc</td>
<td>This port is used by Platform API. Use the <code>ipfilter</code> command to block the port.</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SNMP</td>
<td>Disable the SNMP service on the remote host if you do not use it, or filter incoming UDP packets going to this port.</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Use the <code>ipfilter</code> command to block the port.</td>
</tr>
<tr>
<td>512</td>
<td>TCP</td>
<td>exec</td>
<td></td>
</tr>
<tr>
<td>513</td>
<td>TCP</td>
<td>login</td>
<td></td>
</tr>
<tr>
<td>514</td>
<td>TCP</td>
<td>shell</td>
<td></td>
</tr>
<tr>
<td>897</td>
<td>TCP</td>
<td></td>
<td>This port is used by the Platform API. Disable this port using the <code>configure</code> command.</td>
</tr>
</tbody>
</table>

Configuring for the SSL protocol

Fabric OS 4.4.0 and later supports secure sockets layer (SSL) protocol, which provides secure access to a fabric through Web-based management tools like Web Tools. SSL support is a standard Fabric OS feature.

Switches configured for SSL grant access to management tools through hypertext transfer protocol-secure links (which begin with `https://`) instead of standard links (which begin with `http://`).

SSL uses Public Key Infrastructure (PKI) encryption to protect data transferred over SSL connections. PKI is based on digital certificates obtained from an Internet Certificate Authority (CA), which acts as the trusted key agent.

Certificates are based on the switch IP address or fully qualified domain name (FQDN), depending on the issuing CA. If you change a switch IP address or FQDN after activating an associated certificate, you may have to obtain and install a new certificate. Check with the CA to verify this possibility, and plan these types of changes accordingly.

Browser and Java support

Fabric OS supports the following Web browsers for SSL connections:
- Internet Explorer (Microsoft Windows)
- Mozilla (Solaris and Red Hat Linux)

In countries that allow the use of 128-bit encryption, you should use the latest version of your browser. For example, Internet Explorer 6.0 and later supports 128-bit encryption by default. You can display the encryption support (called “cipher strength”) using the Internet Explorer `Help:About` menu option. If you are running an earlier version of Internet Explorer, you may be able to download an encryption patch from the Microsoft website at [http://www.microsoft.com](http://www.microsoft.com).

You should upgrade to the Java 1.5.0_06 Plug-in on your management workstation. To find the Java version that is currently running, open the Java console and look at the first line of the window.

For more details on levels of browser and Java support, see the Web Tools Administrator’s Guide.
Summary of SSL procedures

You configure for SSL by obtaining, installing, and activating digital certificates for SSL support. Certificates are required on all switches that are to be accessed through SSL.

You also need to install a certificate in the Java Plug-in on the management workstation, and you may need to add a certificate to your Web browser.

Configuring for SSL involves these major steps, which are shown in detail in the next sections.

1. Choose a Certificate Authority (CA).
2. Generate the following items on each switch:
   a. A public/private key (**secCertUtil genkey** command).
   b. A certificate signing request (CSR) (**secCertUtil gencsr** command) and store the CSR on an FTP server (**secCertUtil export** command).
3. Obtain the certificates from the CA.
   You can request a certificate from a CA through a Web browser. After you request a certificate, the CA either sends certificate files by e-mail (public) or gives access to them on a remote host (private). Typically, the CA provides the certificate files listed in Table 20.
   
   **Table 20** SSL certificate files
   
<table>
<thead>
<tr>
<th>Certificate file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name.crt</td>
<td>The switch certificate.</td>
</tr>
<tr>
<td>nameRoot.crt</td>
<td>The root certificate. Typically, this certificate is already installed in the browser, but if not, you must install it.</td>
</tr>
<tr>
<td>nameCA.crt</td>
<td>The CA certificate. It needs to be installed in the browser to verify the validity of the server certificate or server validation fails.</td>
</tr>
</tbody>
</table>

4. On each switch, install and then activate the certificate.
5. If necessary, install the root certificate to the browser on the management workstation.
6. Add the root certificate to the Java Plug-in keystore on the management workstation.

Choosing a CA

To ease maintenance and allow secure out-of-band communication between switches, consider using one CA to sign all management certificates for a fabric. If you use different CAs, management services operate correctly, but the Web Tools Fabric Events button is unable to retrieve events for the entire fabric.

Each CA (for example, Verisign or GeoTrust) has slightly different requirements; for example, some generate certificates based on IP address, while others require an FQDN, and most require a 1024-bit public/private key while some may accept a 2048-bit key. Consider your fabric configuration, check CA websites for requirements, and gather all the information that the CA requires.

Generating a public/private key

Perform this procedure on each switch.

1. Connect to the switch and log in as admin.
2. Enter this command to generate a public/private key pair:
   ```
   switch:admin> seccertutil genkey
   ```
   The system reports that this process will disable secure protocols, delete any existing CSR, and delete any existing certificates.
3. Respond to the prompts to continue and select the key size:
   ```
   Continue (yes, y, no, n): [no] y
   Select key size [1024 or 2048]: 1024
   Generating new rsa public/private key pair
   Done.
   ```
IMPORTANT: HP recommends selecting 1024 in most cases. CA support for the 2048-bit key size is limited.

Generating and storing a CSR

After generating a public/private key, perform this procedure on each switch.

1. Connect to the switch and log in as admin.
2. Enter this command:
   ```
   switch:admin> seccertutil gencsr
   ```
3. Enter the requested information:
   ```
   Country Name (2 letter code, eg, US): US
   State or Province Name (full name, eg, California): California
   Locality Name (eg, city name): San Jose
   Organization Name (eg, company name): Brocade
   Organizational Unit Name (eg, department name): Eng
   Common Name (Fully qualified Domain Name, or IP address): 192.1.2.3
   Generating CSR, file name is: 192.1.2.3.csr
   Done.
   ```

   Your CA may require specific codes for Country, State or Province, Locality, Organization, and Organizational Unit names. Make sure that your spelling is correct and matches the CA requirements. If the CA requires that the Common Name be specified as an FQDN, make sure that the fully qualified domain name is set on the domain name server.

4. Enter this command to store the CSR:
   ```
   switch:admin> seccertutil export
   ```
5. Enter the requested information:
   ```
   Select protocol [ftp or scp]: ftp
   Enter IP address: 192.1.2.3
   Enter remote directory: path_to_remote_directory
   Enter Login Name: your account
   Enter Password: your password
   Success: exported CSR.
   ```

   If you are set up for secure file copy protocol, you can select it; otherwise, select **ftp**. Enter the IP address of the switch on which you generated the CSR. Enter the remote directory name of the FTP server to which the CSR is to be sent. Enter your account name and password on the server.

Obtaining certificates

Check the instructions on the CA website; then, perform this procedure for each switch.

1. Generate and store the CSR as described in “Generating and storing a CSR” on page 89.
2. Open a Web browser window on the management workstation and go to the CA website. Follow the instructions to request a certificate. Locate the area in the request form into which you are to paste the CSR.
3. Through a Telnet window, connect to the switch and log in as admin.
4. Enter this command:
   ```
   switch:admin> seccertutil showcsr
   ```

   The contents of the CSR are displayed.

5. Locate the section that begins with “BEGIN CERTIFICATE REQUEST” and ends with “END CERTIFICATE REQUEST”.
6. Copy and paste this section (including the BEGIN and END lines) into the area provided in the request form; then, follow the instructions to complete and send the request.
It may take several days to receive the certificates. If the certificates arrive by e-mail, save them to an FTP server. If the CA provides access to the certificates on an FTP server, make note of the path name and make sure you have a login name and password on the server.

Installing a switch certificate

Perform this procedure on each switch.

1. Connect to the switch and log in as admin.
2. Enter this command:

   ```
   switch:admin> seccertutil import
   ```
3. Select a protocol, enter the IP address of the host on which the switch certificate is saved, and enter your login name and password:

   ```
   Select protocol [ftp or scp]: ftp
   Enter IP address: 192.10.11.12
   Enter remote directory: path_to_remote_directory
   Enter certificate name (must have ".crt" suffix): 192.1.2.3.crt
   Enter Login Name: your_account
   Enter Password: ****
   Success: imported certificate [192.1.2.3.crt].
   ```

   To use this certificate, run the configure command to activate it. The certificate is downloaded to the switch.

Activating a switch certificate

1. Enter the configure command
2. When the ssl attributes comes up, type y
3. Respond to the prompts that apply to SSL certificates:

   - SSL attributes: Enter y or yes.
   - Certificate File: Enter the name of the switch certificate file: for example, 192.1.2.3.crt.
   - CA Certificate File: If you want the CA name to be displayed in the browser window, enter the name of the CA certificate file; otherwise, skip this prompt.
   - Select length of crypto key: Enter the encryption key length (40, 56, or 128).
   - HTTP attributes: Enter yes.
   - Secure HTTP enabled: Enter yes.

For example:

```config
Configure...
System services (yes, y, no, n): [no]
ssl attributes (yes, y, no, n): [no] yes
Certificate File. (filename or none): [10.33.13.182.crt] 192.1.2.3.crt
CA Certificate File. (filename or none): [none]
Select length of crypto key.
(Valid values are 40, 56, and 128.): (40..128) [128]
http attributes (yes, y, no, n): [no] yes
HTTP Enabled (yes, y, no, n): [yes] no
Secure HTTP Enabled (yes, y, no, n): [no] yes
```

After you exit the configure command, the HTTP daemon restarts automatically to handle HTTPS requests.
Configuring the browser

The root certificate may already be installed on your browser, but if not, you must install it. To see whether it is already installed, check the certificate store on your browser.

The next procedures are guides for installing root certificates to Internet Explorer and Mozilla browsers. For more detailed instructions, refer to the documentation that came with the certificate.

To check and install root certificates on Internet Explorer:

1. From the browser Tools menu, select Internet Options.
2. Click the Content tab.
3. Click Certificates.
4. Click the Intermediate certification authorities or Trusted Root certification authorities tabs and scroll the lists to see if the root certificate is listed. If it is listed, you do not need to install it, forgo the remainder of this procedure.
5. If the certificate is not listed, click Import.
6. Follow the instructions in the Certificate Import wizard to import the certificate.

To check and install root certificates on Mozilla:

1. From the browser Edit menu, select Preferences.
2. In the left pane of the Preferences window, expand the Privacy & Security list and select Certificates.
3. In the right pane, click Manage Certificates.
4. In the next window, click the Authorities tab.
5. Scroll the authorities list to see if the root certificate is listed. (For example, its name may have the form nameRoot.crt.) If it is listed, you do not need to install it; forgo the remainder of this procedure.
6. If the certificate is not listed, click Import.
7. Browse to the certificate location and select the certificate. (For example, select nameRoot.crt.)
8. Click Open and follow the instructions to import the certificate.

Installing a root certificate to the Java plug-in

For information on Java requirements, see “Browser and Java support” on page 87.

This procedure is a guide for installing a root certificate to the Java Plug-in on the management workstation. If the root certificate is not already installed to the plug-in, you should install it. For more detailed instructions, refer to the documentation that came with the certificate and to the Sun Microsystems website, www.sun.com.

1. Copy the root certificate file from its location on the FTP server to the Java Plug-in bin. For example, the bin location may be:
   C: \program files\java\j2re1.5.0_06\bin
2. Open a command prompt window and change directory to the Java Plug-in bin.
3. Enter the keytool command and respond to the prompts:
   c:\Program Files\Java\j2re1.5.0_06\bin> keytool -import -alias RootCert
   -file RootCert.crt -keystore ..\lib\security\RootCerts
   Enter keystore password: changeit
   Owner: CN=Brocade, OU=Software, O=Brocade Communications, L=San Jose, ST=California, C=US
   Issuer: CN=Brocade, OU=Software, O=Brocade Communications, L=San Jose, ST=California, C=US
   Serial number: 0
   Certificate fingerprints:
Trust this certificate? [no]: yes
Certificate was added to keystore

In the example, changeit is the default password and RootCert is an example root certificate name.

Displaying and deleting certificates

Table 21 summarizes the commands for displaying and deleting certificates. For details on the commands, see the Fabric OS Command Reference.

Table 21  Commands for displaying and deleting SSL certificates

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>secCertUtil show</td>
<td>Displays the state of the SSL key and a list of installed certificates</td>
</tr>
<tr>
<td>secCertUtil show filename</td>
<td>Displays the contents of a specific certificate</td>
</tr>
<tr>
<td>secCertUtil showcsr</td>
<td>Displays the contents of a CSR</td>
</tr>
<tr>
<td>secCertUtil delete filename</td>
<td>Deletes a specified certificate</td>
</tr>
<tr>
<td>secCertUtil delcsr</td>
<td>Deletes a CSR</td>
</tr>
</tbody>
</table>

Troubleshooting certificates

If you receive messages in the browser or in a pop-up window when logging in to the target switch using HTTPS, refer to Table 22 for recommended actions you can take.

Table 22  SSL messages and actions

<table>
<thead>
<tr>
<th>Message</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The page cannot be displayed</td>
<td>The SSL certificate is not installed correctly or HTTPS is not enabled correctly. Make sure that the certificate has not expired, that HTTPS is enabled, and that certificate file names are configured correctly.</td>
</tr>
<tr>
<td>The security certificate was issued by a company you have not chosen to trust....</td>
<td>The certificate is not installed in the browser. Install it as described in “Configuring the browser” on page 91.</td>
</tr>
<tr>
<td>The security certificate has expired or is not yet valid</td>
<td>Either the certificate file is corrupted or it needs to be updated. Click View Certificate to verify the certificate content. If it is corrupted or out of date, obtain and install a new certificate.</td>
</tr>
<tr>
<td>The name on the security certificate is invalid or does not match the name of the site file</td>
<td>The certificate is not installed correctly in the Java Plug-in. Install it as described in “Installing a root certificate to the Java plug-in” on page 91.</td>
</tr>
<tr>
<td>This page contains both secure and nonsecure items. Do you want to display the nonsecure items?</td>
<td>Click No in this pop-up window. The session opens with a closed lock icon on the lower-right corner of the browser, indicating an encrypted connection.</td>
</tr>
</tbody>
</table>
Configuring for SNMP

You can configure for the automatic transmission of SNMP information to management stations. SNMPv3 and SNMPv1 are supported.

The configuration process involves configuring the SNMP agent and configuring SNMP traps. The following commands are used in the process:

- Use the `configure` command to set the security level. You can specify no security, authentication only, or authentication and privacy.
- Use the `snmpConfig` command to configure the SNMP agent and traps for SNMPv3 or SNMPv1 configurations.
- If necessary for backward compatibility, you can use these legacy commands to configure for SNMP v1:
  - Use the `agtCfgShow`, `agtCfgset`, and `agtCfgDefault` commands to configure the SNMPv1 agent.
  - Use the `snmpMibCapSet` command to filter at the trap level.

The SNMP trap configuration specifies the MIB trap elements to be used to send information to the SNMP management station. There are two main MIB trap choices:

- Brocade-specific MIB trap
  Associated with the Brocade-specific MIB (SW-MIB), this MIB monitors Brocade (HP) switches specifically.
- FibreAlliance MIB trap
  Associated with the FibreAlliance MIB (FA-MIB), this MIB manages SAN switches and devices from any company that complies with FibreAlliance specifications.

If you use both SW-MIB and FA-MIB, you may receive duplicate information. You can disable the FA-MIB, but not the SW-MIB.

You can also use these additional MIBs and their associated traps:

- FICON-MIB (for FICON environments)
- SW-EXTRAP
  Includes the swSsn (Software Serial Number) as a part of Brocade SW traps.

For information on Brocade MIBs, see the Fabric OS MIB Reference.

For information on the specific commands used in these procedures, see online help or the Fabric OS Command Reference.

Setting the security level

Use the `configure` command to set the security level (called “SNMP attributes”). You can specify no security, authentication only, or authentication and privacy. For example, to configure for authentication and privacy:

```
Stealth200E:admin> configure
Not all options will be available on an enabled switch.
To disable the switch, use the "switchDisable" command.
Configure...

System services (yes, y, no, n): [no]
ssl attributes (yes, y, no, n): [no]
rpdc attributes (yes, y, no, n): [no]
cfgload attributes (yes, y, no, n): [no] y
Enforce secure config Upload/Download (yes, y, no, n): [no]
Enforce signature validation for firmware (yes, y, no, n): [no]
```

Fabric OS 6.x administrator guide  93
webtools attributes (yes, y, no, n): [no]
System (yes, y, no, n): [no]

No changes.

Using the snmpConfig command

4. Use the `snmpConfig --set` command to change either the SNMPv3 or SNMPv1 configuration. You can also change access control, MIB capability, and system group.

Sample SNMPv3 configuration

```
switch:admin> snmpconfig --set snmpv3

SNMPv3 user configuration:
User (rw): [snmpadmin1] adminuser
  Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1
  New Auth Passwd:
  Verify Auth Passwd:
  Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]: (1..2) [2] 1
  New Priv Passwd:
  Verify Priv Passwd:
User (rw): [snmpadmin2] shauser
  Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 2
  New Auth Passwd:
  Verify Auth Passwd:
  Priv Protocol [DES(1)/noPriv(2)]: (1..2) [2] 1
  New Priv Passwd:
  Verify Priv Passwd:
User (rw): [snmpadmin3] nosec
  Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
  Priv Protocol [DES(1)/noPriv(2)]: (2..2) [2]
  User (ro): [snmpuser1]
  Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (3..3) [3]
  Priv Protocol [DES(1)/noPriv(2)]: (2..2) [2]
User (ro): [snmpuser2]
  Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (3..3) [3]
  Priv Protocol [DES(1)/noPriv(2)]: (2..2) [2]
User (ro): [snmpuser3]
  Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (3..3) [3]
  Priv Protocol [DES(1)/noPriv(2)]: (2..2) [2]

SNMPv3 trap recipient configuration:
  Trap Recipient's IP address in dot notation: [0.0.0.0] 192.168.45.90
  UserIndex: (1..6) [1]
  Trap recipient Severity level : (0..5) [0] 4
  Trap Recipient's IP address in dot notation: [0.0.0.0] 192.168.45.92
  UserIndex: (1..6) [2]
  Trap recipient Severity level : (0..5) [0] 2
  Trap Recipient's IP address in dot notation: [0.0.0.0]
  Trap Recipient's IP address in dot notation: [0.0.0.0]
  Trap Recipient's IP address in dot notation: [0.0.0.0]
Committing configuration...done.
```
Sample SNMPv1 configuration

switch:admin> snmpconfig --set snmpv1

SNMP community and trap recipient configuration:
Community (rw): [Secret C0de] admin
Trap Recipient's IP address in dot notation: [0.0.0.0] 10.32.225.1
Trap recipient Severity level: (0..5) [0] 1
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address in dot notation: [10.32.225.2]
Trap recipient Severity level: (0..5) [1]
Community (rw): [private]
Trap Recipient's IP address in dot notation: [10.32.225.3]
Trap recipient Severity level: (0..5) [2]
Community (ro): [public]
Trap Recipient's IP address in dot notation: [10.32.225.4]
Trap recipient Severity level: (0..5) [3]
Community (ro): [common]
Trap Recipient's IP address in dot notation: [10.32.225.5]
Trap recipient Severity level: (0..5) [4]
Community (ro): [FibreChannel]
Trap Recipient's IP address in dot notation: [10.32.225.6]
Trap recipient Severity level: (0..5) [5]
Committing configuration...done.

Sample accessControl configuration

switch:admin> snmpconfig --set accessControl

SNMP access list configuration:
Access host subnet area in dot notation: [0.0.0.0] 192.168.0.0
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0] 10.32.148.0
Read/Write? (true, t, false, f): [true] f
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0] 10.33.0.0
Read/Write? (true, t, false, f): [true] f
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Committing configuration...done.

Sample mibCapability configuration

supp_dcx_218:admin> snmpconfig --show mibcapability

FE-MIB: YES
SW-MIB: YES
FA-MIB: YES
FICON-MIB: YES
HA-MIB: YES
FCIP-MIB: YES
ISCSI-MIB: NO
SW-TRAP: YES
swFCPortScn: YES
swEventTrap: YES
swFabricWatchTrap: YES
swTrackChangesTrap: YES
FA-TRAP: YES
Configuring standard security features

connUnitStatusChange: YES
connUnitEventTrap: YES
connUnitSensorStatusChange: YES
connUnitPortStatusChange: YES
SW-EXTTRAP: NO
FICON-TRAP: YES
linkRNIDDeviceRegistration: YES
linkRNIDDeviceDeRegistration: YES
linkLIRRLisenerAdded: YES
linkLIRRLisenerRemoved: YES
linkRLIRFailureIncident: YES
HA-TRAP: YES
fruStatusChanged: YES
cpStatusChanged: YES
fruHistoryTrap: YES
FCIP-TRAP: NO

Sample systemGroup configuration (default)

switch:admin> snmpconfig --default systemGroup
*****
This command will reset the agent's system group configuration back
to factory default
*****
sysDescr = Fibre Channel Switch
sysLocation = End User Premise
sysContact = Field Support
authTraps = 0 (OFF)

*****
Are you sure? (yes, y, no, n): [no] y

Configuring secure file copy

You can use the configure command to specify that secure file copy (SCP) is used for configuration uploads and downloads.

For example:

switch:admin> configure

Not all options will be available on an enabled switch.
To disable the switch, use the "switchDisable" command.

Configure...

System services (yes, y, no, n): [no] n
ssl attributes (yes, y, no, n): [no] n
http attributes (yes, y, no, n): [no] n
snmp attributes (yes, y, no, n): [no] n
rpcd attributes (yes, y, no, n): [no] n
cfgload attributes (yes, y, no, n): [no] y

Enforce secure config Upload/Download (yes, y, no, n): [no]
Enforce signature validation for firmware (yes, y, no, n):

[no]switch:admin>
4 Configuring advanced security features

This chapter provides information and procedures for configuring advanced Fabric OS security features such as Access Control List (ACL) policies, authentication policies, and IP Filtering for HP’s Fibre Channel switches.

NOTE: Run all commands, with the suggested role, in this chapter by logging in to Administrative Domain (AD) 255 or, if Administrative Domains have not been implemented, log in to AD 0.

About access control list (ACL) policies

Fabric OS provides the following policies:

- **Fabric Configuration Server** (FCS) policy—Used to restrict which switches can change the configuration of the fabric.
- **Device Connection Control** (DCC) policies—Used to restrict which Fibre Channel device ports can connect to which Fibre Channel switch ports.
- **Switch Connection Control** (SCC) policy—Used to restrict which switches can join with a switch.
- **IP Filter Policy** (IPFilter) policy—Used to filter traffic based on IP addresses.

Each supported policy is identified by a specific name, and only one policy of each type can exist (except for DCC policies). Policy names are case-sensitive and must be entered in all uppercase.

How the ACL policies are stored

The policies are stored in a local database. The database contains the ACL policies types of FCS, DCC, SCC, and IPFilter. The number of policies that may be defined is limited by the size of the database. FCS, SCC and DCC policies are all stored in the same database.

When a Fabric OS 6.0 switch joins the fabric containing only pre-6.0 switches, the policy database size limit is restricted to the Fabric OS version’s lowest database size. Table 23 shows the Fabric OS version and its associated database size restriction. Distribution of any of the given policies to pre-6.0 switches would fail if the size of the database being distributed is greater than the lowest database size in the fabric. In a fabric with only Fabric OS 6.0 switches present, the limit for security policy database size would be set to 1Mb. In this case, the pre-6.0 switches cannot join the fabric if the fabric security database size is greater than their Fabric OS database size.

<table>
<thead>
<tr>
<th>Fabric OS version</th>
<th>Security database size</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4</td>
<td>256K</td>
</tr>
<tr>
<td>5.1, 5.2, 5.3</td>
<td>256K</td>
</tr>
<tr>
<td>6.0</td>
<td>1Mb</td>
</tr>
</tbody>
</table>

The policies are grouped by state and type. A policy can be in either of the following states:

- **Active**—The policy is being enforced by the switch.
- **Defined**—The policy has been set up but is not enforced.

A group of policies is called a **Policy Set**. Each switch has the following two sets:

- **Active policy set**—Contains ACL policies being enforced by the switch.
- **Defined policy set**—Contains a copy of all ACL policies on the switch.

When a policy is activated, the defined policy either replaces the policy with the same name in the active set or becomes a new active policy. If a policy appears in the defined set but not in the active set, the policy was saved but has not been activated. If a policy with the same name appears in both the defined
and active sets but they have different values, then the policy has been modified but the changes have not been activated.

**Admin Domain considerations:** ACL management can be done on AD255 and in AD0 only if other there are no user-defined Admin Domains. Both AD0 (when no other user-defined Admin Domains exist) and AD255 provide an unfiltered view of the fabric.

**Identifying policy members**

Specify the FCS, DCC and SCC policy members by device port WWN, switch WWN, Domain IDs, or switch names, depending on the policy. The valid methods for specifying policy members are listed in Table 24.

**Table 24  Valid methods for specifying policy members**

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Device port WWN</th>
<th>Switch WWN</th>
<th>Domain ID</th>
<th>Switch name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCS_POLICY</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DCC_POLICY_1nn</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SCC_POLICY</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Configuring ACL policies**

All policy modifications are saved in volatile memory until those changes are saved or activated. You can create multiple sessions to the switch from one or more hosts. It is recommended to make changes from one switch only to avoid having multiple transactions from occurring.

The FCS, SCC and DCC policies in Secure Fabric OS are not interchangeable with Fabric OS FCS, SCC and DCC policies. Uploading and saving a copy of the Fabric OS configuration after creating policies is strongly recommended. Use the `configUpload` command to upload a copy of the configuration file. For more information on how to use this command, see the “Maintaining Configurations” on page 131.

**NOTE:** All changes, including the creation of new policies, are saved and activated on the local switch only—unless the switch is in a fabric that has a strict or tolerant fabric-wide consistency policy for the ACL policy type for SCC or DCC. See “Distributing the policy database” on page 121 for more information on the database settings and fabric-wide consistency policy.

Use the instructions in the following sections to manage common settings between two or more of the DCC, FCS, and SCC policies. For instructions relating to a specific policy, refer to the appropriate section.

- “Displaying ACL policies” on page 101
  Displays a list of all active and defined ACL policies on the switch.
- “Saving changes to ACL policies” on page 108
  Save changes to memory without actually implementing the changes within the fabric or to the switch. This saved but inactive information is known as the “defined policy set.”
- “Activating changes to ACL policies” on page 108
  Simultaneously save and implement all the policy changes made since the last time changes were activated. The activated policies are known as the “active policy set.”
- “Adding a member to an existing policy” on page 108
  Add one or more members to a policy. The aspect of the fabric covered by each policy is closed to access by all devices and switches that are not listed in that policy.
- “Removing a member from an ACL policy” on page 109
  Remove one or more members from a policy. If all members are removed from a policy, that aspect of the fabric becomes closed to all access.
- “Deleting an ACL policy” on page 109
  Delete an entire policy; deleting a policy opens up that aspect of the fabric to all access.
Displaying ACL policies

Use the `secPolicyShow` command to display the active and defined policy sets. Additionally, in a defined policy set, policies created in the same login session also appear but these policies are automatically deleted if the user logs out without saving. The following example shows a switch that has no SCC, DCC, and FCS policies.

To display the ACL policies:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type the `secPolicyShow` command:

```
switch:admin> secPolicyShow
```

```
ACTIVE POLICY SET

DEFINED POLICY SET
```

Configuring an FCS policy

Fabric Configuration Server (FCS) policy in base Fabric OS may be performed on a local switch basis and may be performed on any switch in the fabric with Fabric OS 6.0.0 or later. Any switch with a pre-5.3.0 version of Fabric OS cannot be included in the FCS list.

The FCS policy is not present by default, but must be created using the command `secPolicyCreate` using CLI or from a management interface. When the FCS policy is created, the WWN of the local switch is automatically included in the FCS list. Additional switches can be included in the FCS list by invoking the `secPolicyAdd` command or using a manageability interface. The first switch in the list becomes the primary FCS switch.

Only the primary FCS switch is allowed to modify and distribute the database within the fabric. Automatic distribution is supported and you can either configure the switches in your fabric to accept the FCS policy using the `fddcfg --fabswideset` command or manually distribute the FCS policy using the `distribute -p` command. Changes made to the FCS policy are saved to permanent memory only after the changes have been saved or activated; they can be aborted later if you have set your fabric to distribute the changes manually.

### Table 25  FCS policy states

<table>
<thead>
<tr>
<th>Policy state</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>No active policy</td>
<td>Any switch can perform fabric wide configuration changes.</td>
</tr>
<tr>
<td>Active policy with one entry</td>
<td>A primary FCS switch is designated (local switch), but there are no backup FCS switches. If the primary FCS switch becomes unavailable for any reason, the fabric is left without an FCS switch.</td>
</tr>
<tr>
<td>Active policy with multiple entries</td>
<td>A primary FCS switch and one or more backup FCS switches are designated. If the primary FCS switch becomes unavailable, the next switch in the list becomes the primary FCS switch.</td>
</tr>
</tbody>
</table>

The FCS policy is designed to accommodate mixed fabric environments that contain switches with pre-5.3.0 and later versions of Fabric OS. By setting the configuration parameters to accept fabric

---

**Fabric OS 6.x administrator guide  101**
distribution, Fabric OS 6.0.0 switches may enforce FCS policy and perform database distribution among 5.3.0 and 6.0.0 switches while still allowing pre-5.3.0 switches to join the fabric.

- Distribution to pre-5.3.0 switches with specific Domain IDs
  When specific Domain IDs are given for the distribution, all domains must be on a switch with Fabric OS 5.3.0 or later. If one of the domains is pre-5.3.0 the distribution operation will fail.

- Distribution to pre-5.3.0 switches using the wild card (*) character
  When the wild card character is specified, distribution succeeds even if the fabric contains pre-5.3.0 switches. However, the FCS database will be sent only to switches with a Fabric OS of 5.2.0 or later in the fabric and not to pre-5.2.0 switches. Fabric OS 5.2.0 switches receive the distribution and will ignore the FCS database.

**FCS policy restrictions**

The backup FCS switches normally cannot modify the policy. However, if the primary FCS switch in the policy list is not reachable, then a back-up FCS switch will be allowed to modify the policy.

Once an FCS policy is configured and distributed across the fabric, only the primary FCS switch can perform certain operations. Operations which affect fabric wide configuration are allowed only from the primary FCS switch. Backup and non-FCS switches cannot perform security, zoning and AD operations that affect the fabric configuration. The following error message are returned if a backup or non-FCS switch tries to perform these operations.

"Can only execute this command on the primary FCS switch."

Operations that do not affect the fabric configuration, such as show or local switch commands, would be allowed on back-up and non-FCS switches.

FCS enforcement applies only for user-initiated fabric wide operations. Internal fabric data propagation because of a fabric merge is not blocked. Consequently, a new switch which joins the FCS enabled fabric could still propagate the AD and zone database.

**Table 26** shows the commands for switch operations for a Primary FCS enforcement.

**Table 26  Switch operations**

<table>
<thead>
<tr>
<th>Allowed on FCS switches</th>
<th>Allowed on all switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>secPolicyAdd (Allowed on all switches for SCC/DCC policies as long as it is not fabric-wide)</td>
<td>secPolicyShow</td>
</tr>
<tr>
<td>secPolicyCreate (Allowed on all switches for SCC/DCC policies as long as it is not fabric-wide)</td>
<td>fddcfg -localaccept/localreject</td>
</tr>
<tr>
<td>secPolicyDelete (Allowed on all switches for SCC/DCC policies as long as its not fabricwide)</td>
<td>userconfig, Passwd, Passwdcfg (Fabric-wide distribution is not allowed from a backup or non-FCS switch.)</td>
</tr>
<tr>
<td>secPolicyRemove (Allowed on all switches for SCC/DCC policies as long as its not fabricwide)</td>
<td>secPolicyActivate</td>
</tr>
<tr>
<td>fddcfg --fabwideset</td>
<td>secPolicySave</td>
</tr>
<tr>
<td>Any fabric-wide commands</td>
<td>secPolicyAbort</td>
</tr>
<tr>
<td>All zoning commands except the show commands</td>
<td>SNMP commands</td>
</tr>
<tr>
<td>All AD commands</td>
<td>configupload</td>
</tr>
<tr>
<td></td>
<td>Any local-switch commands</td>
</tr>
<tr>
<td></td>
<td>Any AD command that does not affect fabric-wide configuration</td>
</tr>
</tbody>
</table>

FCS enforcement does not apply to pre-5.3.0 switches and they will be able to initiate all operations.
Overview of steps to create and manage the FCS policies

Whether your intention is to create new FCS policies or manage your current FCS policies, you must follow certain steps to ensure the domains throughout your fabric have the same policy.

The local-switch WWN cannot be deleted from the FCS policy.

1. Set the pre-6.0 switches in the fabric to accept the FCS policy using the `fddcfg --localaccept/localreject` command.
2. Create the FCS policy using the `secPolicyCreate` command.
3. Activate the policy using the `secPolicyActivate` command.
4. If your switches are set to accept distribution of the policies, you can use the `distribute -p` command to either send the policies to intended domains, or the wild card (*) character to send the policies to all switches.

To create an FCS policy:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type `secPolicyCreate "FCS_POLICY", "member;...;member"`.
   - `member` indicates a switch that is eligible to become a primary or back-up FCS switch. Specify switches by WWN, Domain ID, or switch name. Enter the wild card (*) character to indicate all the switches in the fabric.
   - For example, to create an FCS policy that allows a switch with Domain ID 2 to become a primary FCS and Domain ID 4 to become a backup FCS:
     ```
     switch:admin> secpolicycreate "FCS_POLICY", "2;4"
     FCS_POLICY has been created
     ```

To save or activate the new policy, enter either the `secPolicySave` or the `secPolicyActivate` command. Once the policy has been activated you can distribute the policy.

**NOTE:** FCS policy should be consistent across the fabric. If the policy is inconsistent in the fabric, then you will not be able to perform any fabric-wide configurations from the primary FCS.

Modifying the Primary FCS

To fail over to a new Primary switch, use the `secPolicyFCSMove` command to change the order in which switches are listed in the FCS policy.

To modify the order of FCS switches:

1. Log in to the primary FCS switch using an account assigned to the admin role.
2. Type `secPolicyShow "Defined", "FCS_POLICY"`.
   - This displays the WWNs of the current primary FCS switch and backup FCS switches.
3. Type `secPolicyFCSMove`; then provide the current position of the switch in the list and the desired position at the prompts.
   - Alternatively, enter `secPolicyFCSMove "From, To"`. From is the current position in the list of the FCS switch and To is the desired position in the list for this switch.
For example, to move a backup FCS switch from position 2 to position 3 in the FCS list, using interactive mode:

```
primaryfcs:admin> secpolicyfcsmove
Pos Primary WWN DIdswName.
=================================================
1 Yes 10:00:00:60:69:10:02:181switch5.
2 No 10:00:00:60:69:00:00:5a2switch60.
3 No 10:00:00:60:69:00:00:133switch73.
Please enter position you’d like to move from : (1..3) [1]
Please enter position you’d like to move to : (1..3) [1]
```

```
DEFINED POLICY SET
FCS_POLICY
Pos PrimaryWWN DIdswName
____________________________________________________
1 Yes 10:00:00:60:69:10:02:181switch5.
2 No 10:00:00:60:69:00:00:133switch73.
3 No 10:00:00:60:69:00:00:5a2switch60.
____________________________________________________
```

4. Type `secPolicyActivate`.

**Distributing an FCS policy**

The FCS policy can be automatically distributed using the `fddcfg --fabwideset` command or it can be manually distributed to the switches using the `distribute -p` command. Each switch that receives the FCS policy must be configured to receive the policy. To configure the switch to accept distribution of the FCS policy, refer to “Configuring the database distribution settings” on page 122.

Switches in the fabric are designated as either a Primary FCS, backup FCS, or non-FCS switch. Database distributions may be initiated from only the primary FCS switch. FCS policy configuration and management is performed using the command line or a manageability interface.

Only the primary FCS switch is allowed to distribute the database. The FCS policy may need to be manually distributed across the fabric using the `distribute -p` command if there is no support for automatic distribution in a mixed environment with 5.3.0 and pre-5.3.0 switches. Since this policy is distributed manually, the command `fddcfg --fabwideset` is used to distribute a fabric-wide consistency policy for FCS policy in an environment consisting of only Fabric OS 6.0 switches.

FCS enforcement for the `distribute` command is handled differently for FCS and other databases in an FCS fabric:

- For an FCS database, the enforcement allows any switch to initiate the distribution. This is to support FCS policy creation specifying a remote switch as Primary.
- For other database distributions, only the primary FCS switch can initiate the distribution.

There will be FCS enforcement at the receiving switch, so the switch will verify whether the distribution is coming from the primary FCS switch before accepting it. Distribution is accepted only if it is coming from a primary FCS switch. Distribution of FCS policy can still be accepted from a backup FCS switch if the Primary is not reachable or from a non-FCS switch if the Primary FCS and none of the backup FCS switches are reachable. To learn more about how to distribute policies, refer to “Distributing ACL policies to other switches” on page 123.

**NOTE:** The FCS policy distribution is allowed to be distributed from a switch in the FCS list. However, if none of the FCS switches in the existing FCS list are reachable, receiving switches will accept distribution from any switch in the fabric.

Local switch configuration parameters are needed to control whether a switch accepts or rejects distributions of FCS policy and whether the switch is allowed to initiate distribution of an FCS policy. A configuration parameter controls whether the distribution of the policy is accepted or rejected on the local
switch. Setting the configuration parameter to **accept** indicates distribution of the policy will be accepted and distribution may be initiated using the `distribute -p` command. Setting the configuration parameter to **reject** indicates the policy distribution is rejected and the switch may not distribute the policy.

The default value for the distribution configuration parameter is **accept**, which means the switch accepts all database distributions and is able to initiate a distribute operation for all databases.

### Table 27  Distribution policy states

<table>
<thead>
<tr>
<th>Fabric OS</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0 and 5.3.0 configured to accept</td>
<td>Target switch accepts distribution and fabric state change occurs.</td>
</tr>
<tr>
<td>6.0 and 5.3.0 configured to reject</td>
<td>Target switch explicitly rejects the distribution and the operation fails. The entire transaction is aborted and no fabric state change occurs.</td>
</tr>
<tr>
<td>5.2.0 switch (not configured as it does not support this)</td>
<td>Target switch receives distribution but ignores FCS policy database.</td>
</tr>
<tr>
<td>Pre-5.2.0</td>
<td>No distribution is initiated as pre-5.2.0 versions do not support this operation.</td>
</tr>
</tbody>
</table>

### Configuring a DCC policy

Multiple DCC policies can be used to restrict which device ports can connect to which switch ports. The devices can be initiators, targets, or intermediate devices such as SCSI routers and loop hubs. By default, all device ports are allowed to connect to all switch ports; no DCC policies exist until they are created.

Each device port can be bound to one or more switch ports; the same device ports and switch ports may be listed in multiple DCC policies. After a switch port is specified in a DCC policy, it permits connections only from designated device ports. Device ports that are not specified in any DCC policies are allowed to connect only to switch ports that are not specified in any DCC policies.

When a DCC violation occurs, the related port is automatically disabled and must be re-enabled using the `portEnable` command.

The procedure used to create a DCC policy is described after Table 28, which shows the possible DCC policy states.

### Table 28  DCC policy states

<table>
<thead>
<tr>
<th>Policy state</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>No policy</td>
<td>Any device can connect to any switch port in the fabric.</td>
</tr>
<tr>
<td>Policy with no entries</td>
<td>Any device can connect to any switch port in the fabric. An empty policy is the same as no policy.</td>
</tr>
<tr>
<td>Policy with entries</td>
<td>If a device WWN is specified in a DCC policy, that device is only allowed access to the switch if connected by a switch port listed in the same policy. If a switch port is specified in a DCC policy, it only permits connections from devices that are listed in the policy. Devices with WWNs that are not specified in a DCC policy are allowed to connect to the switch at any switch ports that are not specified in a DCC policy. Switch ports and device WWNs may exist in multiple DCC policies. Proxy devices are always granted full access and can connect to any switch port in the fabric.</td>
</tr>
</tbody>
</table>

### DCC policy restrictions

The following restrictions apply when using DCC policies:

- Some older private-loop HBAs do not respond to port login from the switch and are not enforced by the DCC policy. This does not create a security problem because these HBAs cannot contact any device outside of their immediate loop.
- DCC policies cannot manage or restrict iSCSI connections, that is, an FC Initiator connection from an iSCSI gateway.
• You cannot manage proxy devices with DCC policies. Proxy devices are always granted full access, even if the DCC policy has an entry that restricts or limits access of a proxy device.

Creating a DCC policy

DCC policies must follow the naming convention “DCC_POLICY_nnn,” where nnn represents a unique string. The maximum length is 30 characters, including the prefix DCC_POLICY_. To save memory and improve performance, one DCC policy per switch or group of switches is recommended.

Device ports must be specified by port WWN. Switch ports can be identified by the switch WWN, Domain ID, or switch name followed by the port or area number. To specify an allowed connection, enter the device port WWN, a semicolon, and the switch port identification.

The following methods of specifying an allowed connection are possible:

• deviceportWWN;switchWWN (port or area number)
• deviceportWWN;domainID (port or area number)
• deviceportWWN;switchname (port or area number)

To create a DCC policy:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type secPolicyCreate “DCC_POLICY_nnn”, “member;...;member”.
   DCC_POLICY_nnn is the name of the DCC policy; nnn is a string consisting of up to 19 alphanumeric or underscore characters to differentiate it from any other DCC policies.
   The member contains device or switch port information: deviceportWWN;switch(port) where:

   deviceportWWN The WWN of the device port.
   switch The switch WWN, Domain ID, or switch name. The port can be specified by port or area number. Designating ports automatically includes the devices currently attached to those ports. The ports can be specified using any of the following syntax methods:

   (*) Selects all ports on the switch.
   (1-6) Selects ports 1 through 6.
   [*] Selects all ports and all devices attached to those ports.
   [3, 9] Selects ports 3 and 9 and all devices attached to those ports.
   [1-3, 9] Selects ports 1, 2, 3, 9, and all devices attached to those ports.
   “*” This can be used to indicate DCC lockdown. This will create a unique policy for each port in the fabric, locking it down to the device connected or creating an empty policy to disallow any device to be connected to it. This can be done only when there are no other DCC policies defined on the switch.

3. To save or activate the new policy, enter either the secPolicySave or the secPolicyActivate command.
   If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see “Saving changes to ACL policies” on page 108 and “Activating changes to ACL policies” on page 108.
Examples of creating DCC policies

To create the DCC policy "DCC_POLICY_server" that includes device 11:22:33:44:55:66:77:aa and port 1 and port 3 of switch domain 1:

```
switch:admin> secpolicycreate "DCC_POLICY_server",
DCC_POLICY_server has been created
```

To create the DCC policy "DCC_POLICY_storage" that includes device port WWN 22:33:44:55:66:77:11:bb, all ports of switch domain 2, and all currently connected devices of switch domain 2:

```
switch:admin> secpolicycreate "DCC_POLICY_storage",
DCC_POLICY_storage has been created
```

To create the DCC policy "DCC_POLICY_abc" that includes device 33:44:55:66:77:11:22:cc and ports 1 through 6 and port 9 of switch domain 3:

```
switch:admin> secpolicycreate "DCC_POLICY_abc",
DCC_POLICY_abc has been created
```


```
switch:admin> secpolicycreate "DCC_POLICY_example",
DCC_POLICY_example has been created
```

Creating an SCC policy

Fabric OS 5.2.0 and later support an SCC policy in Fabric OS. The SCC policy is used to restrict which switches can join the fabric. Switches are checked against the policy each time an E_Port-to-E_Port connection is made. The policy is named SCC_POLICY and accepts members listed as WWNs, Domain IDs, or switch names. Only one SCC policy can be created.

By default, any switch is allowed to join the fabric; the SCC policy does not exist until it is created. When connecting a Fibre Channel router to a fabric or switch that has an active SCC policy, the front domain of the Fibre Channel router must be included in the SCC policy.

SCC policy states are shown in Table 29.

**Table 29  SCC policy states**

<table>
<thead>
<tr>
<th>Policy state</th>
<th>SCC policy enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>No active policy</td>
<td>All switches can connect to the switch with the specified policy.</td>
</tr>
<tr>
<td>Active policy that has no members</td>
<td>All neighboring switches are segmented.</td>
</tr>
<tr>
<td>Active policy that has members</td>
<td>The neighboring switches not specified in the SCC policy are segmented.</td>
</tr>
</tbody>
</table>

To create an SCC policy:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type `secPolicyCreate "SCC_POLICY", "member;...;member"`

   `member` indicates a switch that is permitted to join the fabric. Specify switches by WWN, Domain ID, or switch name. Enter an asterisk (*) to indicate all the switches in the fabric.
For example, to create an SCC policy that allows switches that have Domain IDs 2 and 4 to join the fabric:

```bash
switch:admin> secpolicycreate "SCC_POLICY", "2;4"
SCC_POLICY has been created
```

3. To save or activate the new policy, enter either the `secPolicySave` or the `secPolicyActivate` command.

If neither of these commands is entered, the changes are lost when the session is logged out. For more information about these commands, see “Saving changes to ACL policies” on page 108 and “Activating changes to ACL policies” on page 108.

### Saving changes to ACL policies

You can save changes to ACL policies without activating them by entering the `secPolicySave` command. This saves the changes to the defined policy set. Until the `secPolicySave` or `secPolicyActivate` command is issued, all policy changes are in volatile memory only and are lost if the switch reboots or the current session is logged out.

To save changes without activating the policies:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type the `secPolicySave` command.

```bash
switch:admin> secpolicysave
```

### Activating changes to ACL policies

Implement changes to the ACL policies using the `secPolicyActivate` command. This saves the changes to the active policy set and activates all policy changes since the last time the command was issued. You cannot activate policies on an individual basis; all changes to the entire policy set are activated by the command. Until a `secPolicySave` or `secPolicyActivate` command is issued, all policy changes are in volatile memory only and are lost upon rebooting.

To activate changes:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type the `secPolicyActivate` command:

```bash
switch:admin> secpolicyactivate
About to overwrite the current Active data.
ARE YOU SURE (yes, y, no, n): [no] y
```

### Adding a member to an existing policy

Add members to the ACL policies by using the `secPolicyAdd` command. As soon as a policy has been activated, the aspect of the fabric managed by that policy is enforced.

To add a member to an existing policy:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type `secPolicyAdd “policy_name”, “member;...;member”`

   where `policy_name` is the name of the ACL policy, `member` is the item to be added to the policy as identified by IP address, switch Domain ID, device or switch WWN, or switch name.

3. To implement the change immediately, enter the `secPolicyActivate` command.

   For example, to add a member to the SCC_POLICY using the switch WWN:

```bash
switch:admin> secpolicyadd "SCC_POLICY", "12:24:45:10:0a:67:00:40"
```

   Member(s) have been added to SCC_POLICY.


```bash
```
Removing a member from an ACL policy

To remove a member from an ACL policy:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type secPolicyRemove "policy_name", "member; ... ; member".
   where policy_name is the name of the ACL policy. member is the device or switch to be removed
   from the policy, identified by IP address, switch Domain ID, device or switch WWN, or switch name.
3. To implement the change immediately, enter the secPolicyActivate command.
   For example, to remove a member that has a WWN of 12:24:45:10:0a:67:00:40 from SCC_POLICY:
   switch:admin> secpolicyremove "SCC_POLICY", "12:24:45:10:0a:67:00:40"
   Member(s) have been removed from SCC_POLICY.

Deleting an ACL policy

To delete an ACL policy:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type secPolicyDelete "policy_name".
   where policy_name is the name of the ACL policy.
3. To implement the change immediately, enter the secPolicyActivate command.
   switch:admin> secpolicydelete "DCC_POLICY_ALL"
   About to delete policy Finance_Policy.
   Are you sure (yes, y, no, n):[no] y
   Finance_Policy has been deleted.

Aborting all uncommitted changes

Use the secPolicyAbort command to abort all ACL policy changes that have not yet been saved.

To abort all unsaved changes:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Type the secPolicyAbort command:
   switch:admin> secpolicyabort
   Unsaved data has been aborted.
   All changes since the last time the secPolicySave or secPolicyActivate commands were
   entered are aborted.

Configuring the authentication policy for fabric elements

By default, Fabric OS 6.0.0 uses DH-CHAP or FCAP protocols for authentication. These protocols use
shared secrets and digital certificates, based on switch WWN and public key infrastructure (PKI)
technology to authenticate switches. Authentication automatically defaults to FCAP if both switches are
configured to accept FCAP protocol in authentication.

**NOTE:** The fabric authentication feature is available in base Fabric OS. No license is required.

You can configure a switch with Fabric OS 5.3.0 or later to use Diffie-Hellman challenge handshake
authentication protocol (DH-CHAP) for device authentication. Use the authUtil command to configure
the authentication parameters used by the switch. When you configure DH-CHAP authentication, you also
must define a pair of shared secrets known to both switches as a secret key pair. Figure 1 on page 110
illustrates how the secrets are configured. A secret key pair consists of a local secret and a peer secret. The
local secret uniquely identifies the local switch. The peer secret uniquely identifies the entity to which the
local switch authenticates. Every switch can share a secret key pair with any other switch or host in a
fabric.

In order to use DH-CHAP authentication, a secret key pair has to be configured on both switches. To use
FCAP on both switches, PKI certificates have to be installed. You can use the command
authutil --set <fcap|dhchap> to set the authentication protocol which can then be verified using the command authutil --show CLI.

**NOTE:** The standards-compliant DH-CHAP and FCAP authentication protocols are not compatible with the SLAP protocol that was the only protocol supported in earlier Fabric OS releases 4.2, 4.1, 3.1, 2.6.x.

Fabric OS 6.0.0 switch-to-switch authentication implementation is fully backward compatible with 3.2, 4.2, 4.4, 5.0, 5.1, 5.2, and 5.3.0.

Use secAuthSecret to set a shared secret on the switch. When configured, the secret key pair are used for authentication. Authentication occurs whenever there is a state change for the switch or port. The state change can be due to a switch reboot, a switch or port disable and enable, or the activation of a policy.

![Key database on switch](image)

**Key database on switch**
- Local secret A
- Peer secret B

![Key database on switch](image)

**Key database on switch**
- Local secret B
- Peer secret A

**Figure 1** DH-CHAP authentication

If you use DH-CHAP authentication, then a secret key pair must be installed only in connected fabric elements. However, as connections are changed, new secret key pairs must be installed between newly connected elements. Alternatively, a secret key pair for all possible connections may be initially installed, enabling links to be arbitrarily changed while still maintaining a valid secret key pair for any new connection.

The switch authentication (AUTH) policy initiates DH-CHAP/FCAP authentication on all E_Ports. This policy is persistent across reboots, which means authentication will be initiated automatically on ports or switches brought online if the policy is set to activate authentication. The AUTH policy is distributed using the distribute command. The automatic distribution of the AUTH policy is not supported.

The default configuration directs the switch to attempt FCAP authentication first, DH-CHAP second. The switch may be configured to negotiate FCAP, DH-CHAP, or both.

The DH group is used in the DH-CHAP protocol only. The FCAP protocol exchanges the DH group information, but does not use it.

The AUTH policy is designed to accommodate mixed fabric environments that contain Fabric OS 6.0.0 and pre-6.0.0 switches. The policy states PASSIVE and OFF allow connection from Fabric OS 6.0.0 switches to pre-6.0.0 switches. These policy states do not allow switches to send the authentication negotiation and therefore continue with the rest of port initialization.

**E_Port authentication**

The authentication (AUTH) policy allows you to configure the DH-CHAP authentication on the switch. By default the policy is set to PASSIVE and you can change the policy using the authutil command. All changes to the AUTH policy are effective. This includes starting authentication on all E_Ports on the local switch if the policy is changed to ON or ACTIVE, and clearing the authentication if the policy is changed to OFF. The authentication configurations will be effective only on subsequent E_ and F_Port initialization.

A secret key pair has to be installed prior to changing the policy. The policy can be configured as follows:

$authutil --policy -sw <ON|ACTIVE|PASSIVE|OFF>
**WARNING!** If data input has not been completed and a failover occurs, the command is terminated without completion and the entire user input is lost.

If data input has completed, the enter key pressed, and a failover occurs, data may or may not be replicated to the other CP depending on the timing of the failover. Log in to the other CP after the failover is complete and verify the data was saved. If data was not saved, run the command again.

**ON:** Setting the AUTH policy to ON means that strict authentication is enforced on all E_Ports. If the connecting switch does not support authentication or the policy is switched to the OFF state, the ISL is disabled.

During switch initialization, authentication begins automatically on all E_Ports. In order to enforce this policy fabric wide, the fabric needs to have Fabric OS 5.3.0 or later switches only. The switch disables the port if it is connected to a switch which does not support authentication. Regardless of the policy, the E_Port is disabled if the DH-CHAP or FCAP protocol fails to authenticate each other.

**ACTIVE:** In this state the switch is more tolerant and can connect to a switch with any type of policy. During switch initialization, authentication begins on all E_Ports, but the port is not disabled if the connecting switch does not support authentication or the AUTH policy is turned to the OFF state.

The authentication begins automatically during the E_Port initialization. A switch with this policy can safely connect to pre-6.0 switches, since it continues E_Port initialization if the connecting switch does not support authentication. The switches with firmware pre-3.2.0 do not support FCAP/DH-CHAP authentication, so an E_Port initializes without authentication. The switches with firmware version 3.2.0 and later respond to authentication negotiation and participate in FCAP/DH-CHAP handshaking. Regardless of the policy, the E_PORT gets disabled if the DH-CHAP or FCAP protocol fails to authenticate each other.

**PASSIVE (default):** In the PASSIVE state the switch does not initiate authentication, but participates in authentication if the connecting switch initiates authentication.

The switch will not start authentication on E_Ports, but accepts the incoming authentication requests, and will not disable if the connecting switch does not support authentication or the policy is turned to the OFF state. This is the safest policy for switches connecting to pre-5.3.0 switches. That means 5.3.0 and later switches can have authentication enabled and this will not impact the pre-5.3.0 switches. By default the pre-5.3.0 switches act as passive switches, since they accept incoming authentication requests. Regardless of the policy, E_Port is disabled if the DH-CHAP or FCAP protocol fails to authenticate each other.

**OFF:** This setting turns off the policy. The switch will not support authentication and rejects any authentication negotiation request from another switch. A switch with the policy turned OFF cannot be connected to a switch with the policy turned ON. The ON state is strict and disables the port if any switch rejects the authentication. DH-CHAP shared secrets must be configured before changing the policy from the OFF to the ON state.

The behavior of the policy between two adjacent switches is defined as follows. If the policy is ON or active, the switch will send an authentication negotiation request to the connecting switch. If the connecting switch does not support authentication or the policy is OFF, the request will be rejected. Once the authentication negotiation succeeds, the DH-CHAP authentication will be initiated. If DH-CHAP authentication fails, the port is disabled and this is applicable in all modes of the policy.
Device authentication policy

Device authentication policy can also be categorized as an HBA authentication policy. Fabric wide distribution of the device authentication policy is not supported since the device authentication requires manual interaction in setting the HBA shared secrets and switch shared secrets, and most of the HBAs do not support the defined DH groups for use in the DH-CHAP protocol.

By default the switch will be in OFF state, which means the switch will clear the security bit in the FLOGI (fabric login). The authutil command provides an option to change the device policy mode to select PASSIVE policy, which means switch responds to authentication from any device and does not initiates authentication to devices.

```
$authutil --policy -dev <off|passive>
```

The following lists available policy modes and properties.

**OFF (Default):** Authentication is not required. Even if device sends FLOGI with security bit set, switch accepts the FLOGI with security bit OFF. In this case, switch assumes no further authentication requests from device.

**PASSIVE:** Authentication is optional. If the attached device is capable of doing the authentication then the switch participates in authentication; otherwise it will form an F_Port without authentication.

In PASSIVE mode, an F_Port will be disabled if the HBA shared secret does not match with the secret installed on the switch. If the secret provided by the switch does not match the secrets installed on the HBA then the HBA will disable the port on its side. On any authentication handshaking rejection, the switch will disable the F_Port with reason “Authentication rejected”.

Since the F_Port authentication requires DH-CHAP protocol, selecting the PASSIVE mode will be blocked if only FCAP protocol is selected as the authentication protocol. Similarly de-selecting the DH-CHAP protocol from the authentication protocol list will be blocked if the device authentication is set to PASSIVE.

Auth policy restrictions

Fabric OS 5.1.0 implementation of DH-CHAP/FCAP does not support integration with RADIUS. All fabric element authentication configurations are performed on a local switch basis.

Device authentication policy supports devices that are connected to the switch in point-to-point manner and is visible to the entire fabric. The following are not supported:

- Public loop devices
- Single private devices
- Private loop devices
- Mixed public and private devices in loop
- NPIV devices
- FICON channels
- Configupload/download will not be supported for the following AUTH attributes: auth type, hash type, group type.

Supported configurations

The following HBAs support authentication:

- Emulex LP11000 (Tested with Storport Miniport 2.0 windows driver)
- Qlogic QLA2300 (Tested with Solaris 5.04 driver)
Selecting authentication protocols

Use the authUtil command to perform the following tasks:

- Display the current authentication parameters
- Select the authentication protocol used between switches
- Select the Diffie-Hellman (DH) group for a switch

Run the authUtil command on the switch you want to view or change. Options for specifying which DH group you want to use include:

- 00 – DH Null option
- 01 – 1024 bit key
- 02 – 1280 bit key
- 03 - 1536 bit key
- 04 – 2048 bit key

This section illustrates using the authUtil command to display the current authentication parameters and to set the authentication protocol to DH-CHAP.

To view the current authentication parameter settings for a switch:

1. Log in to the switch using an account assigned to the admin role.
2. On a switch running Fabric OS 6.0, type authUtil --show.

Output similar to the following is displayed:

```
AUTH TYPE      HASH TYPE   GROUP TYPE
--------------------------------------
fcap,dhcaps    sha1,md5     0, 1, 2, 3, 4
```

Switch Authentication Policy: PASSIVE
Device Authentication Policy: OFF

To set the authentication protocol used by the switch to DH-CHAP:

1. Log in to the switch using an account assigned to the admin role.
2. On a switch running Fabric OS 4.x or 5.x, type authUtil --set -a dhchap; on a switch running Fabric OS 3.x, type authUtil "--set -a dhchap".

Output similar to the following is displayed:

```
Authentication is set to dhchap.
```

When using DH-CHAP, make sure that you configure the switches at both ends of a link.

**NOTE:** If you set the authentication protocol to DH-CHAP, have not yet configured shared secrets, and authentication is checked (for example, you enable the switch), switch authentication fails.

Re-authenticating ports

Use the command authutil to re-initiate the authentication on selected ports. It provides flexibility to initiate authentication for specified E_Ports, set of E_Ports, and all E_Ports on the switch. This command will not work on Private, Loop, NPIV and FICON devices. The command authutil can re-initiate authentication only if the device was previously authenticated. If the authentication fails because shared secrets do not match, the port is disabled.

This command works independently of the authentication policy; this means you can initiate the authentication even if the switch is in PASSIVE mode. This command is used to restart authentication after changing the DH-CHAP group, hash type, and shared secret between a pair of switches.
△ WARNING!  This command may bring down the E_Port(s) if the DH-CHAP shared secrets are not installed correctly.

To re-authenticate E_Ports:

1. Log in to the switch using an account assigned to the admin role.
2. On a switch running Fabric OS 5.3.0 and later, type the following command:
   $authutil --authinit <slot/port_number(s)|allE>

Example
   $authutil --authinit 2,3,4

Example
   $authutil --authinit allE (all E_ports in the switch)

For directors, use the slot/port format for specifying the port number.

Example
   $authutil --authinit 1/1, 1/2

Managing secret key pairs

When you configure the switches at both ends of a link to use DH-CHAP for authentication, you must also define a secret key pair—one for each end of the link. Use the secAuthSecret command to perform the following tasks:

• View the WWN of switches with a secret key pair
• Set the secret key pair for switches
• Remove the secret key pair for one or more switches

Note the following characteristics of a secret key pair:

• The secret key pair must be set up locally on every switch. The secret key pair are not distributed fabric-wide.
• If a secret key pair are not set up for a link, authentication fails. The “Authentication Failed” (reason code 05h) error will be reported and logged.
• The minimum length of a shared secret is 8 bytes and the maximum length is 40 bytes.

This section illustrates using the secAuthSecret command to display the list of switches in the current switch’s shared secret database and to set the secret key pair for the current switch and a connected switch. See the Fabric OS Command Reference for more details on the secAuthSecret command.

NOTE:  When setting a secret key pair, note that you are entering the shared secrets in plain text. Use a secure channel (for example, SSH or the serial console) to connect to the switch on which you are setting the secrets.

To view the list of secret key pairs in the current switches database:

1. Log in to the switch using an account assigned to the admin role.
2. On a switch running Fabric OS 4.x, 5.x, or 6.0, type secAuthSecret --show; on a switch running Fabric OS 3.x, type secAuthSecret "--show".

The output displays the WWN, Domain ID, and name (if known) of the switches with defined shared secrets:

<table>
<thead>
<tr>
<th>WWN</th>
<th>DId</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00:00:60:69:80:07:52</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td>10:00:00:60:69:80:07:5c</td>
<td>1</td>
<td>switchA</td>
</tr>
</tbody>
</table>
To set a secret key pair:

1. Log in to the switch using an account assigned to the admin role.
2. On a switch running Fabric OS 4.x, 5.x, or 6.0, type `secAuthSecret --set`; on a switch running Fabric OS 3.x, type `secAuthSecret "--set"`.

The command enters interactive mode. The command returns a description of itself and needed input; then it loops through a sequence of switch specification, peer secret entry, and local secret entry. To exit the loop, press `Enter` for the switch name; then type `y`.

```
switchA:admin> secAuthSecret --set
```

This command is used to set up secret keys for the DH-CHAP authentication. The minimum length of a secret key is 8 characters and maximum 40 characters. Setting up secret keys does not initiate DH-CHAP authentication. If switch is configured to do DH-CHAP, it is performed whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press Enter to start setting up shared secrets > <cr>

Enter WWN, Domain, or switch name (Leave blank when done): 10:20:30:40:50:60:70:80

Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter WWN, Domain, or switch name (Leave blank when done): 10:20:30:40:50:60:70:81

Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter WWN, Domain, or switch name (Leave blank when done): <cr>
Are you done? (yes, y, no, n): [no] y

Saving data to key store... Done.

3. Disable and enable the ports on a peer switch using the `portDisable` and `portEnable` commands.

Fabric wide distribution of the Auth policy

The AUTH policy can be manually distributed to the fabric using the `distribute` command; there is no support for automatic distribution. Since this policy is distributed manually, you cannot set fabric-wide consistency policy (`fddcfg --fabwideset`) for automatic fabric-wide distribution.

To distribute the AUTH policy, see “To distribute the local ACL policies:” on page 124 for instructions.
Accept distributions configuration parameter

Local Switch configuration parameters are needed to control whether a switch accepts or rejects distributions of the AUTH policy using the distribute command and whether the switch may initiate distribution of the policy. To set the local switch configuration parameter, refer to “Configuring the database distribution settings” on page 122.

IP Filter policy

The IP Filter policy is a set of rules applied to the IP management interfaces as a packet filtering firewall. The firewall permits or denies the traffic to go through the IP management interfaces according to the policy rules.

Fabric OS supports multiple IP Filter policies to be defined at the same time. Each IP Filter policy is identified by a name and has an associated type. Two IP Filter policy types, IPv4 and IPv6, exist to provide separate packet filtering for IPv4 and IPv6. It is not allowed to specify an IPv6 address in the IPv4 filter, or specify an IPv4 address in the IPv6 filter. There can be up to six different IP Filter policies defined. Only one IP Filter policy, however, for each IP Filter policy type, can be activated on the affected management IP interfaces.

Audit messages will be generated for any changes to the IP Filter policies.

The rules in the IP Filter policy are examined one at a time until the end of the list of rules. For performance reasons, the most import rules must be specified at the top.

On a chassis system, changes to persistent IP Filter policies are automatically synchronized to the standby CP when the changes are saved persistently on the active CP to the standby CP. The standby CP will enforce the filter policies to its management interface after policies are synchronized with the active CP.

Creating an IP Filter policy

You can create an IP Filter policy with the specified name and type. The policy created is stored in a temporary buffer, and will be lost if the current command session logs out. The policy name is a unique string composed of a maximum of 20 alpha, numeric, and underscore characters. The names default_ipv4 and default_ipv6 are reserved for default IP Filter policies. The policy name is case insensitive and always stored as lower case. The policy type identifies the policy as an IPv4 or IPv6 filter. There can be a maximum of six IP Filter policies created.

To create an IP Filter policy:

1. Log in to the switch using an account assigned to the admin role.
2. Type in the following command:

   ipfilter --create <policyname> -type <ipv4 | ipv6>

   where <policyname> is the name of the new policy and -type specified as an IPv4 or IPv6 address.

Cloning an IP Filter policy

You can create an IP Filter policy as an exact copy of an existing policy. The policy created is stored in temporary buffer and has the same type and rules as the existing defined or active policy.

To clone an IP Filter policy

1. Log in to the switch using an account assigned to the admin role.
2. Type the following command:

   ipfilter --clone <policyname> -from <src_policyname>

   where <policyname> is the name of the new policy and <src_policyname> is the name of the policy you want to copy.
Displaying an IP Filter policy

Displays the IP Filter policy content for the specified policy name, or all IP Filter policies if policy name is not specified.

For each IP Filter policy, the policy name, type, persistent state and policy rules are displayed. The policy rules are listed by the rule number in ascending order. There is no pagination stop for multiple screens of information. Pipe the output to the more command to achieve this.

If a temporary buffer exists for a IP Filter policy, the --show sub-command displays the content in the temporary buffer, with the persistent state set to no.

To display an IP Filter policy:
1. Log in to the switch using an account assigned to the admin role.
2. Type in the following command:
   
   ipfilter --show <policyname>

   where <policyname> is the name of the policy.

Saving an IP Filter policy

This will save one or all IP Filter policies persistently in the defined configuration. The policy name is optional for this sub-command. If the policy name is given, the IP Filter policy in temporary buffer will be saved; if the policy name is not given, all IP Filter policies in the temporary buffer will be saved. Only the CLI session that owns the updated temporary buffer may run this command. Modification to an active policy cannot be saved without being applied. Hence, the --save sub-command is blocked for the active policies. Use --activate instead.

To save an IP Filter policy:
1. Log in to the switch using an account assigned to the admin role.
2. Type in the following command:

   ipfilter --save [policyname]

   where [policyname] is the name of the policy and is optional.

Activating an IP Filter policy

IP Filter policies are not enforced until they are activated. Only one IP Filter policy per IPv4 and IPv6 type can be active. If there is a temporary buffer for the policy, the policy is saved to the defined configuration and activated at the same time. If there is no temporary buffer for the policy, the policy existing in the defined configuration will become active. The activated policy continues to remain in the defined configuration. The policy to be activated will replace the existing active policy of the same type. Activating the default IP Filter policies will return the IP management interface to its default state. An IP Filter policy without any rule cannot be activated. This sub-command will prompt for a user confirmation before proceeding.

To activate an IP Filter policy:
1. Log in to the switch using an account assigned to the admin role.
2. Type in the following command:

   ipfilter --activate <policyname>

   where <policyname> is the name of the policy.
Deleting an IP Filter policy

You can delete a specified IP Filter policy. Deleting an IP Filter policy will remove it from the temporary buffer. To permanently delete the policy from persistent database, run `ipfilter --save`. An active IP Filter policy cannot be deleted.

To delete an IP Filter policy:

1. Log in to the switch using an account assigned to the admin role.
2. Type in the following command:
   ```
   ipfilter --delete <policyname>
   ```
   where `<policyname>` is the name of the policy.
3. To permanently delete the policy, type the following command:
   ```
   ipfilter --save
   ```

IP Filter policy rules

An IP Filter policy consists of a set of rules. Each rule has an index number identifying the rule. There can be maximum 256 rules within an IP Filter policy.

Each rule contains the following elements:

- **Source Address:** A source IP address or a group prefix.
- **Destination Port:** The destination port number or name, such as Telnet, SSH, HTTP, HTTPS.
- **Protocol:** The protocol type. Supported types are TCP or UDP.
- **Action:** The filtering action taken by this rule, Permit or Deny.

For an IPv4 filter policy, the source address has to be a 32-bit IPv4 address in dot decimal notation. The group prefix has to be a CIDR block prefix representation. For example, 208.130.32.0/24 represents a 24-bit IPv4 prefix starting from the most significant bit. The special prefix 0.0.0.0/0 matches any IPv4 address. In addition, the keyword `any` is supported to represent any IPv4 address.

For an IPv6 filter policy, the source address has to be a 128-bit IPv6 address, in a format acceptable in RFC 3513. The group prefix has to be a CIDR block prefix representation. For example, 12AB:0:0:CD30::/64 represents a 64-bit IPv6 prefix starting from the most significant bit. In addition, the keyword `any` is supported to represent any IPv6 address.

For the destination port, a single port number, or a port number range can be specified. According to IANA (http://www.iana.org), ports 0 to 1023 are well-known port numbers, ports 1024 to 49151 are registered port numbers, and ports 49152 to 65535 are dynamic or private port numbers. Well-known and registered ports are normally used by servers to accept connections, while dynamic port numbers are used by clients.

For an IP Filter policy rule, users can only select port numbers in either the well known or the registered port number range, between 0 and 49151, inclusive. This means that customers have the ability to control how to expose the management services hosted on a switch, but not the ability to affect the management traffic that is initiated from a switch. A valid port number range is represented by a dash, for example 7-30. Alternatively, service names can also be used instead of port number. Table 30 lists the supported service names and their corresponding port number.

**Table 30 Supported services**

<table>
<thead>
<tr>
<th>Service name</th>
<th>Port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>https</td>
<td>443</td>
</tr>
<tr>
<td>rpc</td>
<td>897</td>
</tr>
<tr>
<td>secure rpc</td>
<td>898</td>
</tr>
<tr>
<td>snmp</td>
<td>161</td>
</tr>
<tr>
<td>ssh</td>
<td>22</td>
</tr>
<tr>
<td>sunrpc</td>
<td>111</td>
</tr>
</tbody>
</table>
TCP and UDP protocols are valid selections. Fabric OS 5.3.0 and later does not support configuration to filter other protocols. Implicitly, ICMP type 0 and type 8 packets are always allowed to support ICMP echo request and reply on commands like ping and traceroute. For the action, only “permit” and “deny” are valid.

For every IP Filter policy, the following two rules are always assumed to be appended implicitly to the end of the policy. This is to ensure TCP and UDP traffics to dynamic port ranges is allowed, that way management IP traffic initiated from a switch, such as syslog, radius and ftp, will not be affected.

Table 31  Implicit IP Filter rules

<table>
<thead>
<tr>
<th>Source address</th>
<th>Destination port</th>
<th>Protocol</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>1024-65535</td>
<td>TCP</td>
<td>Permit</td>
</tr>
<tr>
<td>Any</td>
<td>1024-65535</td>
<td>UDP</td>
<td>Permit</td>
</tr>
</tbody>
</table>

A switch with Fabric OS 5.3.0 or later will have a default IP Filter policy for IPv4 and IPv6. The default IP Filter policy cannot be deleted or changed. When an alternative IP Filter policy is activated, the default IP Filter policy becomes deactivated. **Table 32** lists the rules of the default IP Filter policy.

Table 32  Default IP policy rules

<table>
<thead>
<tr>
<th>Rule number</th>
<th>Source address</th>
<th>Destination port</th>
<th>Protocol</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>22</td>
<td>TCP</td>
<td>Permit</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>23</td>
<td>TCP</td>
<td>Permit</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>897</td>
<td>TCP</td>
<td>Permit</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>898</td>
<td>TCP</td>
<td>Permit</td>
</tr>
<tr>
<td>5</td>
<td>Any</td>
<td>111</td>
<td>TCP</td>
<td>Permit</td>
</tr>
<tr>
<td>6</td>
<td>Any</td>
<td>80</td>
<td>TCP</td>
<td>Permit</td>
</tr>
<tr>
<td>7</td>
<td>Any</td>
<td>443</td>
<td>TCP</td>
<td>Permit</td>
</tr>
<tr>
<td>9</td>
<td>Any</td>
<td>161</td>
<td>UDP</td>
<td>Permit</td>
</tr>
<tr>
<td>10</td>
<td>Any</td>
<td>111</td>
<td>UDP</td>
<td>Permit</td>
</tr>
<tr>
<td>11</td>
<td>Any</td>
<td>123</td>
<td>UDP</td>
<td>Permit</td>
</tr>
<tr>
<td>12</td>
<td>Any</td>
<td>600-1023</td>
<td>UDP</td>
<td>Permit</td>
</tr>
</tbody>
</table>

**IP Filter policy enforcement**

An active IP Filter policy is a filter applied to the IP packets through the management interface. IPv4 management traffic will pass through the active IPv4 filter policy, and IPv6 management traffic will pass through the active IPv6 filter policy. The IP Filter policy applies to the incoming (ingress) management traffic only. When a packet arrives, it is compared against each rule, starting from the first rule. If a match is found for the source address, destination port, and protocol, the corresponding action for this rule is taken, and the subsequent rules in this policy will be ignored. If there is no match, then it is compared to the next rule in the policy. This process continues until the incoming packet is compared to all rules in the active policy.
If none of the rules in the policy matches the incoming packet, the two implicit rules will be matched to the incoming packet. If the rules still do not match the packet, the default action, which is to deny, will be taken.

When the IPv4 or IPv6 address for the management interface of a switch is changed through the `ipAddrSet` command or manageability tools, the active IP Filter policies will automatically become enforced on the management IP interface with the changed IP address.

**NOTE:** If a switch is part of a LAN behind a Network Address Translation (NAT) server, depending on the NAT server configuration, the source address in an IP Filter rule may have to be the NAT server address.

### Creating IP Filter policy rules

There can be a maximum of 256 rules created for an IP Filter policy. The change to the specified IP Filter policy is not saved to the persistent configuration until a save or activate sub-command is run.

To add a rule to an IP Filter policy:

1. Log in to the switch using an account assigned to the admin role.
2. Type in the following command:

   ```
ipfilter --addrule <policyname> -rule <rule_number> -sip <source IP> -dp <dest port> -proto <protocol> -act <permit | deny>
   ```

   - `policyname`: Specifies the policy name which is a unique string composed of a maximum of 20 alphanumeric and underscore characters. The names `default_ipv4` and `default_ipv6` are reserved for the default IP Filter policies. The policy name is case-insensitive and always stored as lower case.
   - `rule number`: Enter a valid rule number between 1 and the current maximum rule number plus one.
   - `sip source IP`: Specifies the source IP address. For IPv4 filter type, the address must be a 32-bit address in dot decimal notation, or a CIDR block IPv4 prefix. For IPv6 filter type, the address must be a 128-bit IPv6 address in any format specified by RFC, or a CIDR block IPv6 prefix.
   - `dp destination port`: Specifies the destination port number, or a range of port numbers, or a service name.
   - `proto protocol`: Specifies the protocol type, either TCP or UDP.
   - `act <permit | deny>`: Specifies the permit or deny action associated with this rule.

### Deleting IP Filter policy rules

Deleting a rule in the specified IP Filter policy causes the rules following the deleted rule to shift up in rule order. The change to the specified IP Filter policy is not saved to persistent configuration until a save or activate sub-command is run.

To delete a rule to an IP Filter policy:

1. Log in to the switch using an account assigned to the admin role.
2. Type in the following command:

   ```
ipfilter --delrule <policyname> -rule <rule number>
   ```

### Aborting a switch session transaction

A transaction is associated with a command line or manageability session. It is opened implicitly when the `--create`, `--addrule`, `--delrule`, `--clone`, and `--delete` subcommands are run. The `--transabort`, `--save`, or `--activate` subcommands will explicitly end the transaction owned by the current command line or manageability session. If a transaction is not ended, other command line or manageability sessions are blocked on the sub-commands that would open a new transaction.
To abort a transaction associated with IP Filter:

1. Log in to the switch using an account assigned to the admin role.
2. Type in the following command:
   
   ipfilter --transabort

**IP Filter policy distributions**

The IP Filter policy is manually distributed, using the `distribute --p "IPFILTER"` command. The distribution includes both active and defined IP Filter policies. All policies are combined as a single entity to be distributed and cannot be selectively distributed. However, you may choose the time at which to implement the policy for optimization purposes. If a distribution includes an active IP Filter policy, the receiving switches will activate the same IP Filter policy automatically. When a switch receives IP Filter policies, all uncommitted changes left in its local transaction buffer will be lost, and the transaction will be aborted.

When firmware is upgraded for the first time from pre-5.3.0 to 5.3.0, the default IPv4 and IPv6 filter policies are active. If non-default IP Filter policies are created, and then saved but not activated, and firmware is downgraded to pre-5.3.0, the non-default IP Filter policies are preserved. Subsequently, if the firmware is upgraded again to 5.3.0, the saved IP Filter policies remains present and become visible again. If, however, the default IP Filter policy is not active, a firmware downgrade to pre-5.3.0 is blocked.

Switches with Fabric OS 5.3.0 or later will have the ability to accept or deny IP Filter policy distribution, through the commands `fddCfg --localaccept` or `fddcfg --localreject`. However, automatic distribution of IP Filter policy through Fabric Wide Consistent Policy is not supported in Fabric OS 6.0.0. See “Distributing ACL policies to other switches” on page 123 for more information on distributing the IP Filter policy.

**IP Filter policy restrictions**

In a mixed fabric with Fabric OS 5.3.0 or later and pre-5.3.0 switches, IP Filter policies cannot be distributed from a Fabric OS 6.0.0 switch to a pre-5.3.0 switch. This means that the sending switch will fail `distribute --p "IPFILTER"` operation, if the specified receiving domain list contains switches with Fabric OS 5.2.0 and earlier. When the asterisk (\*) is used as the receiving domain, the sending switch will distribute the IP Filter policies only to switches with Fabric OS 5.3.0 or later.

**Distributing the policy database**

Fabric OS lets you manage and enforce the ACL policy database on either a per-switch or fabric-wide basis. The local switch distribution setting and the fabric-wide consistency policy affect the switch ACL policy database and related distribution behavior.

The ACL policy database is managed as follows:

- **Switch database distribution setting**—Controls whether or not the switch accepts or rejects databases distributed from other switches in the fabric. The `distribute` command sends the database from one switch to another, overwriting the target switch database with the distributed one. To send or receive a database the setting must be accept. For configuration instructions, see “Configuring the database distribution settings” on page 122.

- **Manually distribute an ACL policy database**—Run the `distribute` command to push the local database of the specified policy type to target switches. “Distributing ACL policies to other switches” on page 123.

- **Fabric-wide consistency policy**—Use to ensure that switches in the fabric enforce the same policies. Set a strict or tolerant fabric-wide consistency policy for each ACL policy type to automatically distribute that database when a policy change is activated. If a fabric-wide consistency policy is not set, then the policies are managed on per switch basis. For configuration instructions, see “Setting the consistency policy fabric-wide” on page 124.
Table 33 explains how the local database distribution settings and the fabric-wide consistency policy affect the local database when the switch is the target of a distribution command.

### Table 33 Interaction between fabric-wide consistency policy and distribution settings

<table>
<thead>
<tr>
<th>Distribution setting</th>
<th>Fabric-wide consistency policy</th>
<th>Tolerant</th>
<th>Strict</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject</td>
<td>Database is protected, it cannot be overwritten. May not match other databases in the fabric.</td>
<td>Invalid configuration.¹</td>
<td>Invalid configuration.¹</td>
</tr>
<tr>
<td>Accept (default)</td>
<td>Database is not protected, the database can be overwritten. If the switch initiating a distribute command has a strict or tolerant fabric-wide consistency policy, the fabric-wide policy is also overwritten. May not match other databases in the fabric.</td>
<td>Database is not protected. Automatically distributes activated changes to other 5.20 switches in the fabric. Allows switches running Fabric OS 5.1.x and earlier in the fabric. May not match other databases in the fabric.</td>
<td>Database is not protected. Automatically distributes activated changes to all switches in the fabric. Fabric can only contain switches running Fabric OS 5.2.0 or later. Active database is the same for all switches in the fabric.</td>
</tr>
</tbody>
</table>

¹ Error returned indicating that the distribution setting must be accept before you can set the fabric-wide consistency policy.

### Configuring the database distribution settings

The distribution settings control whether a switch accepts or rejects distributions of databases from other switches and whether or not the switch may initiate a distribution. Configure the distribution setting to reject when maintaining the database on a per-switch basis.

Table 34 lists the databases supported in Fabric OS 5.3.0 and later switches.

### Table 34 Supported policy databases

<table>
<thead>
<tr>
<th>Database type</th>
<th>Database identifier (ID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication policy database</td>
<td>AUTH</td>
</tr>
<tr>
<td>DCC policy database</td>
<td>DCC</td>
</tr>
<tr>
<td>FCS policy database</td>
<td>FCS</td>
</tr>
<tr>
<td>IP Filter policy database</td>
<td>IPFILTER</td>
</tr>
<tr>
<td>Password database</td>
<td>PWD</td>
</tr>
<tr>
<td>SCC policy database</td>
<td>SCC</td>
</tr>
</tbody>
</table>

To display the database distribution settings:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the following command:

```bash
switch:admin> fddcfg --showall
Local Switch Configuration for all Databases:-
  DATABASE - Accept/Reject
  -------------------
    SCC - accept
    DCC - accept
    PWD - accept
    FCS - accept
    AUTH - accept
    IPFILTER - accept
```

Fabric Wide Consistency Policy: ""

To enable local switch protection:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the following command:

```bash
fddCfg --localreject <database_ID>
```

   `localreject` Refuse the databases distributed from other switches. Cannot distribute local
database, manually or automatically, to other switches.

database_id A semicolon-separated list of the local databases to be distributed; see
<Link>Table 34 on page 122 for a list of identifiers.

To disable local switch protection:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the following command:

```bash
fddCfg --localaccept <database_ID>
```

   `localaccept` Default setting. Allows local database to be overwritten with databases
received from other switches. Allows local database to be manually or
automatically distributed to other switches.

database_id A semicolon-separated list of the local databases to be distributed; see
<Link>Table 34 on page 122 for a list of identifiers.

### Distributing ACL policies to other switches

This section explains how to manually distribute local ACL policy databases to Fabric 5.2.0 and later
switches. The distribute command has the following dependencies:

- All target switches must be running Fabric OS 5.2.0 or later.
- All target switches must accept the database distribution (see <Link>“Configuring the database
distribution settings” on page 122).
- The fabric must have a tolerant or no (absent) fabric-wide consistency policy (see <Link>“Setting the
consistency policy fabric-wide” on page 124).

If the fabric-wide consistency policy for a database is strict, the database cannot be manually
distributed. When you set a strict fabric-wide consistency policy for a database, the distribution
mechanism is automatically invoked whenever the database changes.

- The local distribution setting must be accepted. To be able to initiate the distribute command, set the
local distribution to accept.
Table 35 describes how the target switch database distribution settings affect the distribution.

<table>
<thead>
<tr>
<th>Target switch</th>
<th>Distribution</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric OS version</td>
<td>Database setting</td>
<td></td>
</tr>
<tr>
<td>5.1.0 or earlier</td>
<td>NA</td>
<td>Fails</td>
</tr>
<tr>
<td>5.2.0</td>
<td>Reject</td>
<td>Fails</td>
</tr>
<tr>
<td></td>
<td>Accept</td>
<td>Succeeds</td>
</tr>
</tbody>
</table>

To distribute the local ACL policies:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the following command:
   ```
   distribute -p <database_id> -d <switch_list>
   ```

   - `database_id`: A semicolon-separated list of the local databases to be distributed: SCC, DCC, or both.
   - `switch_list`: A semicolon-separated list of switch Domain IDs, switch names, or switch WWN addresses of the target switches that will receive the distribution. Use an asterisk (*) to distribute the database to all Fabric OS 5.2.0 and later switches in the fabric. For example, entering the command: `distribute -p SCC -d ***` distributes the SCC policy to all 5.2.0 and later switches in the fabric.

**Setting the consistency policy fabric-wide**

The fabric-wide consistency policy enforcement setting determines the distribution behavior when changes to a policy are activated. Using the tolerant or strict fabric-wide consistency policy ensures that changes to local ACL policy databases are automatically distributed to other switches in the fabric.

When you set the fabric-wide consistency policy using the `fddCfg` command with the `--fabwideset <database_id>` option, both the fabric-wide consistency policy and specified database are distributed to the fabric. The active policies of the specified databases overwrite the corresponding active and defined policies on the target switches.

Policy changes that are saved but not activated are stored locally until a policy database change is activated. Activating a policy automatically distributes the Active policy set for that policy type (SCC, DCC, or both), to the other switches in the fabric.

**NOTE:** FC routers cannot join a fabric with a strict fabric-wide consistency policy. FC routers do not support the fabric-wide consistency policies.

Table 36 describes the fabric-wide consistency settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>When a policy is activated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absent</td>
<td>null</td>
<td>Database is not automatically distributed to other switches in the fabric.</td>
</tr>
<tr>
<td>Tolerant</td>
<td>&lt;database_id&gt;</td>
<td>All updated and new policies of the type specified (SCC, DCC, or both) are distributed to all Fabric 5.2.0 and later switches in the fabric.</td>
</tr>
<tr>
<td>Strict</td>
<td>&lt;database_id&gt;:S</td>
<td>All updated and new policies of the type specified (SCC, DCC, or both) are distributed to all switches in the fabric.</td>
</tr>
</tbody>
</table>
To display the fabric-wide consistency policy:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `fddCfg --showall` command.

   The following example shows policies for a fabric where no consistency policy is defined.

   ```
   switch:admin> fddcfg --showall
   Local Switch Configuration for all Databases:
   DATABASE  -  Accept/Reject
   ------------------------------
   SCC  -         accept
   DCC  -         accept
   PWD  -         accept
   FCS  -         accept
   AUTH -         accept
   IPFILTER -     accept
   Fabric Wide Consistency Policy: - ""
   ```

   To set the fabric-wide consistency policy:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the following command:

   ```
   fddCfg --fabwideset "<policy_ID>"
   ```

   where `policy_ID` is a semicolon-separated list `database_setting;database_setting` equal to
   - null: Exclude the database ID from the list to set the policy to absent.
   - database_id: Sets a tolerant policy for a database. The database ID is either SCC, DCC, or FCS.
   - database_id:S: Sets the policy to strict. The database ID is either SCC, DCC, or FCS.

   The following example shows how to set a strict SCC and tolerant DCC fabric-wide consistency policy.

   ```
   switch:admin> fddcfg --fabwideset "SCC:S;DCC"
   switch:admin> fddcfg --showall
   Local Switch Configuration for all Databases:
   DATABASE  -  Accept/Reject
   ------------------------------
   SCC  -         accept
   DCC  -         accept
   PWD  -         accept
   FCS  -         accept
   AUTH -         accept
   IPFILTER -     accept
   Fabric Wide Consistency Policy: - "SCC:S;DCC"
   ```

Notes on joining a switch to the fabric

When a switch is joined to a fabric with a tolerant SCC or DCC fabric-wide consistency policy, the joining switch must have a matching tolerant SCC or DCC fabric-wide consistency policy. If the tolerant SCC or DCC fabric-wide consistency policies do not match, the switch can join the fabric, but an error message flags the mismatch. If the tolerant SCC and DCC fabric-wide consistency policies match, the corresponding SCC and DCC ACL policies are compared.

The enforcement of fabric-wide consistency policy involves comparison of only the Active policy set. If the ACL policies match, the switch joins the fabric successfully. If the ACL policies are absent on the switch or on the fabric, the switch joins the fabric successfully, and the ACL policies are copied automatically from where they are present to where they are absent. The Active policies set where they are present overwrite the Active and Defined policies set where they are absent. If the ACL policies do not match, the switch can join the fabric, but an error message flags the mismatch.
Under both conflicting conditions, secPolicyActivate is blocked in the merged fabric. Use fddcfg -fabwideset command to resolve the fabric-wide consistency policy conflicts. Use the distribute command to explicitly resolve conflicting ACL policies.

When a switch is joined to a fabric with a strict SCC or DCC fabric-wide consistency policy, the joining switch must have a matching fabric-wide consistency policy. If the strict SCC or DCC fabric-wide consistency policies do not match, the switch cannot join the fabric and the neighboring E_Ports will be disabled. If the strict SCC and DCC fabric-wide consistency policies match, the corresponding SCC and DCC ACL policies are compared.

The enforcement of fabric-wide consistency policy involves comparison of only the Active policy set. If the ACL policies match, the switch joins the fabric successfully. If the ACL policies are absent either on the switch or on the fabric, the switch joins the fabric successfully, and the ACL policies are copied automatically from where they are present to where they are absent. The Active policy set where it is present overwrites the Active and Defined policy set where it is absent. If the ACL policies do not match, the switch cannot join the fabric and the neighboring E_Ports are disabled.

Use the fddcfg -fabwideset command on either this switch or the fabric to set a matching strict SCC or DCC fabric-wide consistency policy. Use ACL policy commands to delete the conflicting ACL policy from one side to resolve ACL policy conflict. If neither the fabric nor the joining switch is configured with a fabric-wide consistency policy, there are no ACL merge checks required.

The descriptions above also apply to joining two fabrics. In this context, the joining switch becomes a joining fabric.

Matching fabric-wide consistency policies

This section describe the interaction between the databases with active SCC and DCC policies and combinations of fabric-wide consistency policy settings when fabrics are merged.

For example: Fabric A with SCC:S;DCC (strict SCC and tolerant DCC) joins Fabric B with SCC:S;DCC (strict SCC and tolerant DCC), the fabrics can merge as long as the SCC policies match (both are strict).

Table 37 describes the impact of merging fabrics with the same fabric-wide consistency policy that have SCC, DCC, or both policies.

Table 37 Merging fabrics with matching fabric-wide consistency policies

<table>
<thead>
<tr>
<th>Fabric-wide consistency policy</th>
<th>Fabric A ACL policies</th>
<th>Fabric B ACL policies</th>
<th>Merge results</th>
<th>Database copied</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>None</td>
<td>Succeeds</td>
<td>No ACL policies copied.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCC/DCC</td>
<td>Succeeds</td>
<td>No ACL policies copied.</td>
</tr>
<tr>
<td>Tolerant</td>
<td>None</td>
<td>None</td>
<td>Succeeds</td>
<td>No ACL policies copied.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCC/DCC</td>
<td>Succeeds</td>
<td>ACL policies are copied from B to A.</td>
</tr>
<tr>
<td>Strict</td>
<td>None</td>
<td>None</td>
<td>Succeeds</td>
<td>No ACL policies copied.</td>
</tr>
<tr>
<td></td>
<td>SCC/DCC</td>
<td>Succeeds</td>
<td>ACL policies are copied from B to A.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SCC/DCC</td>
<td>Succeeds</td>
<td>No ACL policies copied.</td>
</tr>
<tr>
<td>Different SCC/DCC policies</td>
<td>Different SCC/DCC</td>
<td>Fails</td>
<td>Ports are disabled.</td>
<td></td>
</tr>
</tbody>
</table>

1. To resolve the policy conflict, manually distribute the database you want to use to the switch with the mismatched database. Until the conflict is resolved commands such as fddcfg -fabwideset and secPolicyActivate are blocked.
Non-matching fabric-wide consistency policies

You may encounter one of the following two scenarios:

Merging a fabric with a strict policy to a fabric with an absent, tolerant, or non-matching strict policy. The merge fails and the ports are disabled.

**Table 38** shows merges that are not supported.

**Table 38** Examples of strict fabric merges

<table>
<thead>
<tr>
<th>Fabric-wide consistency policy setting</th>
<th>Expected behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric A</td>
<td>Fabric B</td>
</tr>
<tr>
<td>Strict/Tolerant</td>
<td>- SCC:S;DCC:S</td>
</tr>
<tr>
<td></td>
<td>- SCC;DCC:S</td>
</tr>
<tr>
<td>Strict/Absent</td>
<td>- SCC:S;DCC:S</td>
</tr>
<tr>
<td></td>
<td>- SCC:S</td>
</tr>
<tr>
<td></td>
<td>- DCC:S</td>
</tr>
<tr>
<td>Strict/Strict</td>
<td>- SCC:S</td>
</tr>
<tr>
<td></td>
<td>- DCC:S</td>
</tr>
</tbody>
</table>

Ports connecting switches are disabled.

**Table 39** has a matrix of merging fabrics with tolerant and absent policies.

**Table 39** Fabric merges with tolerant/absent combinations

<table>
<thead>
<tr>
<th>Fabric-wide consistency policy setting</th>
<th>Expected behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric A</td>
<td>Fabric B</td>
</tr>
<tr>
<td>Tolerant/Absent</td>
<td>- SCC;DCC</td>
</tr>
<tr>
<td></td>
<td>- DCC</td>
</tr>
<tr>
<td></td>
<td>- SCC;DCC</td>
</tr>
<tr>
<td></td>
<td>- DCC</td>
</tr>
</tbody>
</table>

Error message logged. Run `fddCfg --fabwiderset "<policy_ID>"` from any switch with the desired configuration to fix the conflict. The `secPolicyActivate` command is blocked until conflict is resolved.

**FIPS support**

Federal information processing standards (FIPS) specifies the security standards to be satisfied by a cryptographic module utilized in the Fabric OS to protect sensitive information in the switch. As part of FIPS 140-2 level 2 compliance passwords, shared secrets and the private keys used in SSL, TLS, and system login need to be cleared out or zeroized. Power-up self tests are executed when the switch is powered on to check for the consistency of the algorithms implemented in the switch. KATs are used to exercise various features of the algorithm and their results are displayed on the console for your reference. Conditional tests are performed whenever RSA key pair is generated. These tests verify the randomness of the deterministic and non-deterministic random number generator (DRNG and non-DRNG). They also verify the consistency of RSA keys with regard to signing and verification and encryption and decryption.
Explicit zeroization can be done at the discretion of the security administrator. These functions clear the passwords and the shared secrets. The following table lists the various keys used in the system that will be zeroized in a FIPS compliant FOS module.

**Table 40  Zeroization behavior**

<table>
<thead>
<tr>
<th>Keys</th>
<th>Zeroization CLI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH Private keys</td>
<td>No CLI required</td>
<td>Keys will be zeroized within code before they are released from memory.</td>
</tr>
<tr>
<td>FCSP Challenge Handshake</td>
<td>secauthsecret --remove</td>
<td>The secauthsecret --remove is used to remove/zeroize the keys.</td>
</tr>
<tr>
<td>Authentication Protocol (CHAP) Secret</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCAP Private Key</td>
<td>pkiremove</td>
<td>The pkiremove command creates the keys, and 'pkiremove' removes/zeroizes the keys.</td>
</tr>
<tr>
<td>SSH Session Key</td>
<td>No CLI required</td>
<td>This is generated for each SSH session that is established to and from the host. It automatically zeroizes on session termination.</td>
</tr>
<tr>
<td>SSH RSA private Key</td>
<td>No CLI required</td>
<td>Key based SSH authentication is not used for SSH sessions.</td>
</tr>
<tr>
<td>RNG Seed Key</td>
<td>No CLI required</td>
<td>/dev/urandom is used as the initial source of seed for RNG. RNG seed key is zeroized on every random number generation.</td>
</tr>
<tr>
<td>Passwords</td>
<td>passwddefault fipscfg --zeroize</td>
<td>This will remove user defined accounts in addition to default passwords for the root, admin, and user default accounts. However only root has permissions for this command. So securityadmin and admin roles need to use fipscfg --zeroize which in addition to removing user accounts and resetting passwords, also does the complete zeroization of the system.</td>
</tr>
<tr>
<td>TLS private keys</td>
<td>seccertutil delkey</td>
<td>The command seccertutil delkey is used to zeroize these keys.</td>
</tr>
<tr>
<td>TLS pre-master secret</td>
<td>No CLI required</td>
<td>Automatically zeroized on session termination</td>
</tr>
<tr>
<td>TLS session key</td>
<td>No CLI required</td>
<td>Automatically zeroized on session termination</td>
</tr>
<tr>
<td>TLS authentication key</td>
<td>No CLI required</td>
<td>Automatically zeroized on session termination</td>
</tr>
<tr>
<td>RADIUS secret</td>
<td>aaaconfig --remove</td>
<td>The aaaconfig --remove zeroizes the secret and deletes a configured server.</td>
</tr>
</tbody>
</table>

Power-up self tests

The self tests are invoked by powering on the switch in FIPS mode and do not require any operator intervention. These tests can also be invoked by the user through a CLI interface.

**NOTE:** Perform power-on self-tests. If any of KAT tests fail, the switch goes into a FIPS Error state which is to reboot the system to single-user mode. You will need to perform a recovery procedure by booting into single-user mode to recover the system.
Conditional tests

These tests are for the random number generators and are executed to verify the randomness of the random number generator. The conditional tests are executed each time prior to using the random number provided by the random number generator.

The results of all self-tests, for both power-up and conditional, are recorded in the system log or are output to the local console. This includes logging both passing and failing results.

To enter into single-user mode:

1. Reboot the switch or Active CP and press **ESC** within four seconds after the following message appears:
   
   Press escape within 4 seconds to enter boot interface.

   On dual CP systems, reboot both active and standby to boot prompt, and execute the following steps on the standby CP as well.

2. **Optional**: If applicable, enter the Boot PROM password.

3. Enter **3** to select **Enter command shell**.

4. From the command prompt, enter the command appropriate for your switch or director:
   
   - HP StorageWorks 4/8 or 4/16 SAN and 4/32 switches, and the 4/256 SAN Director:
     
     boot MEM()0xF0000000 -s
   
   - On the HP StorageWorks DC Director:
     
     setenv OSLoadOptions single boot
   
   - On the 400 MP Router platform:
     
     boot ATA()0xb689f -s

Snapshot of entering into single user mode in the 400 MP Router platform:

Matched board/model ID to platform index 10
Checking system RAM - press any key to stop test

Checking memory address: 00100000

System RAM test using Default POST RAM Test succeeded.

Press escape within 4 seconds to enter boot interface.

1) Start system.
2) Recover password.
3) Enter command shell.

Option? 3

Boot PROM password has not been set.
> printenv
AutoLoad=yes
ENET_MAC=00051E38A087
ENET_Src=10.33.64.253
InitTest=MEM()
LoadIdentifiers=Fabric Operating System;Fabric Operating System
OSLoadOptions=2
OSLoader=ATA()0xb689f;ATA()0x1b0c00
OSRootPartition=hda1;hda2
SkipWatchdog=yes
> boot ATA()0xb689f -s
Booting "Manually selected OS" image.
Entry point at 0x01000000 ...
5. On all platforms, from the shell prompt, enter the following commands:
   ```bash
   mount -o remount,rw,noatime /
   mount /dev/hda2 /mnt
   ```

6. Verify the FIPS configuration by typing the following at the command prompt:
   ```bash
   /fabos/abin/fipscfg --showall
   ```

7. If FIPS mode is ‘Enabled’, reset it by typing the following at the command prompt:
   ```bash
   /fabos/abin/fipscfg --disable fips
   ```

8. If Selftests mode is Enabled/None or Enabled/Pass or Enabled/Failed, reset it by typing the following at the command prompt:
   ```bash
   fipscfg --disable selftests
   ```

9. Reboot the active system by typing the `reboot` command.

10. Login to the switch or Active CP as admin or securityAdmin, and verify that the FIPS and SELFTESTS modes have been reset by typing the `fipscfg --showall` command.

11. On dual CP systems, reboot the standby CP and ensure that the system comes up.

**FIPS mode**

By default, the switch will come up non-FIPS mode. You can run the command `fipscfg --enable`, to enable FIPS mode. Self-tests mode needs to be enabled, before FIPS mode can be enabled. A set of pre-requisites as mentioned in the table below needs to be satisfied for the system to enter FIPS mode. See the Fabric OS Command Reference Manual for additional FIPS related commands.

To be FIPS-compliant, the switch needs to be rebooted. KATs will be run on the reboot. If the KATs are successful, the switch will enter FIPS mode. If KATs fail, then the switch will reboot until the KATs succeed. You will need to access the switch in single-user mode to break the reboot cycle.

Only FIPS compliant algorithms will be run at this stage.

**Table 41** FIPS mode restrictions

<table>
<thead>
<tr>
<th>Features</th>
<th>FIPS mode</th>
<th>Non-FIPS mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root account</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Telnet/SSH access</td>
<td>Only SSH</td>
<td>Telnet and SSH</td>
</tr>
<tr>
<td>SSH algorithms</td>
<td>HMAC-SHA1 (mac) 3DES-CBC, AES128-CBC, AES192-CBC, AES256-CBC (cipher suites)</td>
<td>No restrictions</td>
</tr>
<tr>
<td>HTTP/HTTPS access</td>
<td>HTTPS only</td>
<td>HTTP and HTTPS</td>
</tr>
<tr>
<td>HTTPS protocol/algorithms</td>
<td>TLS/AES128 cipher suite</td>
<td>TLS/AES128 cipher suite (SSL will no longer be supported)</td>
</tr>
<tr>
<td>RPC/secure RPC access</td>
<td>Secure RPC only</td>
<td>RPC and secure RPC</td>
</tr>
<tr>
<td>Secure RPC protocols</td>
<td>TLS - AES128 cipher suite</td>
<td>SSL and TLS – all cipher suites</td>
</tr>
<tr>
<td>SNMP</td>
<td>Read-only operations</td>
<td>Read and write operations</td>
</tr>
</tbody>
</table>
Preparing the switch for FIPS

The following functionalities are blocked in FIPS mode. Therefore, it is important to prepare the switch by disabling these functionalities prior to enabling FIPS.

- The root account is blocked in FIPS mode. Therefore, all root only functionalities will not be available.
- HTTP, Telnet, RPC, SNMP protocols need to be disabled. Once these are blocked, you cannot use these protocols to read or write data from and to the switch
- Configdownload and firmwaredownload using an FTP server will be blocked.

See Table 41 on page 130 for a complete list of restrictions between FIPS and non-FIPS mode.

**IMPORTANT:** Only roles with SecurityAdmin and Admin can enable FIPS mode.

Overview of steps

1. **Optional:** Configure RADIUS server
2. **Optional:** Configure authentication protocols
3. Block Telnet, HTTP, and RPC
4. Disable BootProm access
5. Configure the switch for signed firmware
6. Disable root access
7. Enable FIPS

To enable FIPS mode:

1. Log in to the switch using an account assigned the admin or securityAdmin role.
2. **Optional:** If the switch is set for RADIUS, modify each server to use only *peap-mschapv2* as the authentication protocol using the `aaaconfig --change` or `aaaconfig --remove` command.
3. **Optional:** Set the authentication protocols
   a. Type the following command to set the hash type for MD5 which is used in authentication protocols DHCHAP and FCAP:
      
      ```
      authutil --set -h sha1
      ```
   b. Set the DH group to 1 or 2 or 3 or 4 using `authutil --set -g <n>`, where the DH group is represented by `<n>`.  
4. Block Telnet, HTTP, and RPC using the `ipfilter policy` command.
   You will need to create an IPFilter policy for each protocol.
   a. Create an IP Filter rule for each protocol, see “To create an IP Filter policy:” on page 116.

---

**Table 41** FIPS mode restrictions

<table>
<thead>
<tr>
<th>Features</th>
<th>FIPS mode</th>
<th>Non-FIPS mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH-CHAP/FCAP hashing algorithms</td>
<td>SHA-1</td>
<td>MD5 and SHA-1</td>
</tr>
<tr>
<td>Signed firmware</td>
<td>Mandatory firmware signature validation</td>
<td>Optional firmware signature validation</td>
</tr>
<tr>
<td>Configupload/download/supportsave/firmwaredownload</td>
<td>SCP only</td>
<td>FTP and SCP</td>
</tr>
<tr>
<td>IPSec</td>
<td>Usage of AES-XCBC, MD5 and DH group 1 are blocked</td>
<td>No restrictions</td>
</tr>
<tr>
<td>Radius auth protocols</td>
<td>PEAP-MSCHAPv2</td>
<td>CHAP, PAP, PEAP-MSCHAPv2</td>
</tr>
</tbody>
</table>
b. Add a rule to the IP Filter policy, see “To add a rule to an IP Filter policy:” on page 120. You can use the following modifications to the rule:

```
ipfilter --addrule <policyname> -rule <rule_number> -sip <source_IP> -dp <dest_port> -proto <protocol> -act <deny>
```

- `-sip` option can be given as `any`
- `-dp` option for the port numbers for Telnet, HTTP, and RPC are 23, 80, and 898 respectively
- `-proto` option should be set to `tcp`

c. Activate the IP Filter policy, see “To activate an IP Filter policy:” on page 117.
d. Save the IP Filter policy, see “To save an IP Filter policy:” on page 117.

**Example**

```
ipfilter --createrule http_block_v4 --type ipv4
ipfilter --addrule http_block_v4 -rule 2 -sip any -dp 80 -proto tcp -act deny
ipfilter --activate http_block_v4
ipfilter --save http_block_v4
```

5. Type the following command to block access to the boot PROM:

```
fipscfg --disable bootprom
```

Block boot PROM access before disabling root account.

6. Enable signed firmware by typing the configure command and respond to the prompts as follows:

```
switch:admin> configure
Not all options will be available on an enabled switch.
To disable the switch, use the "switchDisable" command.
Configure...
System services (yes, y, no, n): [no]
...  
cfgload attributes (yes, y, no, n): [no] yes
Enforce secure config Upload/Download (yes, y, no, n): [no]
Enforce firmware signature validation (yes, y, no, n): [no] yes
```

**Example**

```
switch:admin> configure
Not all options will be available on an enabled switch.
To disable the switch, use the "switchDisable" command.
Configure...
System services (yes, y, no, n): [no]
...  
cfgload attributes (yes, y, no, n): [no] yes
Enforce secure config Upload/Download (yes, y, no, n): [no]
Enforce firmware signature validation (yes, y, no, n): [no] yes
```

7. Type the following command to block access to root:

```
userconfig --change root -e no
```

By disabling the root account, RADIUS and LDAP users with root roles are also blocked in FIPS mode.

8. Verify your switch is FIPS ready:

```
fipscfg --verify fips
```

9. Type the command `fipscfg --enable fips`.

10. Reboot the switch.

To disable FIPS mode:

1. Log in to the switch using an account assigned the admin or securityAdmin role.

2. Type the command `fipscfg --disable fips`.

3. Reboot the switch.

4. Enable the root account by following the bootrom:

```
userconfig --change root -e yes
```

5. Enable access to the bootrom:

```
fipscfg --enable bootrom
```
6. Optional: Use the configure command to set switch to use non-signed firmware. By keeping the switch set to use signed firmware, all firmware downloaded to the switch will have to be signed with a key.

7. Disable selftests by typing the following command:

   `fipscfg --disable selftests`

8. Disable IPFilter policies that were created to enable FIPS.


10. Reboot the switch.

To zeroize for FIPS:

1. Log in to the switch using an account assigned the admin or securityAdmin role.
2. Type the command `fipscfg --zeroize`.
3. Reboot the switch.

To display FIPS configuration:

1. Log in to the switch using an account assigned the admin or securityAdmin role.
2. Type the command `fipscfg --showall`.


5 Maintaining configurations

This chapter provides procedures for basic switch configuration maintenance.

Maintaining consistent configuration settings

It is important to maintain consistent configuration settings on all switches in the same fabric because inconsistent parameters (such as inconsistent PID formats) can cause fabric segmentation. As part of standard configuration maintenance procedures, it is recommended that you back up all important configuration data for every switch on a host computer server for emergency reference.

NOTE: For information about AD-enabled switches using Fabric OS 5.2.0 or later, see “Managing administrative domains” on page 143.

Displaying configuration settings

There are two ways to view configuration settings for a switch in an HP StorageWorks fabric:

• Issue the configShow command (less information).

  To display configuration settings using the CLI, connect to the switch, log in as admin, and enter the configShow command at the command line. The configuration settings vary depending on switch model and configuration.

• Issue the configUpload command to upload an ASCII text file from the switch or switch module.

Backing up a configuration

In case the configuration is lost or unintentional changes are made, keep a backup copy of the configuration file. You should keep individual backup files for all switches in the fabric and avoid copying configurations from one switch to another.

The following information is not saved in a backup:

• dnsconfig information  
• passwords

If your setup supports anonymous users, and you log in as an anonymous user, password is still a required field, even though its value may be ignored by the FTP service.

Before beginning, verify that you can reach the FTP server from the switch. Using a Telnet connection, save a backup copy of the configuration file from a logical switch to a host computer.

To upload a configuration file:

1. Verify that the FTP service is running on the host computer.
2. Connect to the switch and log in as admin.
3. Enter the configUpload command. The command becomes interactive and you are prompted for the required information.
4. Respond to the prompts as follows:

- **Protocol (scp or ftp)**: If your site requires the use of Secure Copy, specify scp. Otherwise, specify FTP.
- **Server Name or IP Address**: Enter the name or IP address of the server where the file is to be stored; for example, 192.1.2.3. You can enter a server name if DNS is enabled. For details about the dnsConfig command, see the Fabric OS Command Reference.
- **User Name**: Enter the user name of your account on the server; for example, JohnDoe.
- **File name**: Specify a file name for the backup file; for example, config.txt. Absolute path names can be specified using a forward slash (/). Relative path names create the file in the user’s home directory on UNIX servers, and in the directory where the FTP server is running on Windows servers.
- **Password**: Enter your account password for the server. Note that this is a required field even if you are logged in as an anonymous user; in such cases, the value may be ignored by the FTP service.

The following example shows configUpload run on a switch without Admin Domains:

```
switch:admin> configupload
Protocol (scp or ftp) [ftp]: ftp
Server Name or IP Address [host]: 192.1.2.3
User Name [user]: JohnDoe
File Name [config.txt]: /pub/configurations/config.txt
Password: xxxxx

configUpload complete: All config parameters are uploaded.
```

The following example shows configUpload run on a switch with Admin Domains:

```
switch:AD5:admin> ad --select 5
switch:AD5:admin> configUpload
Protocol (scp or ftp) [ftp]:
Server Name or IP Address [host]: 10.1.2.3
User Name [user]: JohnDoe
File Name [config.txt]: /pub/configurations/config.txt
Password: xxxxx

configUpload complete: Only zoning parameters are uploaded from ad5.
```

5. Store a soft copy of the switch configuration information in a safe place for future reference.

---

NOTE: The configuration file is printable, but you may want to see how many pages will be printed before you send it to the printer.

---

**Troubleshooting configuration upload**

If the configuration upload fails, it may be because of one or more of the following reasons:

- The host name is not known to the switch.
- The host IP address cannot be contacted.
- You do not have configuration upload permission on the switch.
- You do not have permission on the host to perform configuration upload.

Resolve the issue and try the command again.
Restoring switch information

Run the commands listed in Table 42 and save the output in a file format. Store the files in a safe place for emergency reference.

**Table 42** CLI commands to display switch configuration information

<table>
<thead>
<tr>
<th>Command</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>configShow</td>
<td>System configuration parameters and settings, including license information, zoning, and licensing information.</td>
</tr>
<tr>
<td>ipAddrShow</td>
<td>The IP address.</td>
</tr>
<tr>
<td>licenseShow</td>
<td>The license keys you have installed and provides better detail than the license information from the configshow command.</td>
</tr>
<tr>
<td>fosConfig</td>
<td>Fabric OS features.</td>
</tr>
<tr>
<td>iscsiCfg</td>
<td>iSCSI entities.</td>
</tr>
<tr>
<td>iscsiTargetName</td>
<td>The IQN prefix.</td>
</tr>
<tr>
<td>iscsiPortCfg</td>
<td>The iSCSI port parameters.</td>
</tr>
<tr>
<td>isnsCfg</td>
<td>The configuration state of the iSNS client operation.</td>
</tr>
<tr>
<td>fcLunQuery</td>
<td>A list of LUN IDs and LUNs for all accessible targets.</td>
</tr>
<tr>
<td>portCfgEXPort</td>
<td>EX_Port configuration parameters.</td>
</tr>
<tr>
<td>portCfgVEXPort</td>
<td>VEX_Port configuration parameters.</td>
</tr>
<tr>
<td>fcrRouterPortCost</td>
<td>FC router route information</td>
</tr>
<tr>
<td>fcrXlateConfig</td>
<td>A translate (xlate) domain’s Domain ID for both EX_Port-attached fabric and backbone fabric.</td>
</tr>
</tbody>
</table>

Restoring a configuration

Restoring a configuration involves overwriting the configuration on the switch by downloading a previously saved backup configuration file. Make sure that the configuration file you are downloading is compatible with your switch model, because configuration files from other model switches might cause your switch to fail.

The configuration download process is additive, that is, the lines read from the files are added to the current switch configuration. You can change a single configuration variable by downloading a file with that specific variable only. When you do so, all other variables remain unchanged.

If your setup supports anonymous users, and you log in as an anonymous user, **password** is still a required field, even though its value may be ignored by the FTP service.

If a configupload command is issued on a non-FCR platform, FCR-like parameters may be viewed in the uploaded data. This is harmless to the switch and can be ignored.

Configuration download without disabling a switch

Starting in Fabric OS 5.2.0, you can download configuration files to a switch while the switch is enabled, that is, you do not need to disable the switch for changes in SNMP, Fabric Watch, and ACL parameters. When you use the configDownload command, you will be prompted to disable the switch only when necessary. However, if there is any changed parameter that does not belong to SNMP, Fabric Watch, or ACL, then you must disable the switch.

Configuration download without disabling a switch is independent of the hardware platform and supported on all hardware platforms running Fabric OS 5.2.0 and later.

You may attempt to download a configuration file first without disabling the switch. If there is at least one changed parameter outside of SNMP, Fabric Watch, and ACL, you will be prompted to disable the switch before proceeding.
To restore a configuration:

1. Verify that the FTP service is running on the server where the backup configuration file is located.
2. Connect to the switch and log in as admin.
3. If there are any changed parameters in the configuration file that do not belong to SNMP, Fabric Watch, or ACL, disable the switch by entering the `switchDisable` command.
4. Enter the `configDownload` command.
   The command becomes interactive and you are prompted for the required information.
5. Respond to the prompts as follows:
   - **Protocol (scp or ftp)**: If your site requires the use of Secure Copy, specify scp. Otherwise, specify ftp.
   - **Server Name or IP Address**: Enter the name or IP address of the server where the file is stored; for example, 192.1.2.3. You can enter a server name if DNS is enabled.
   - **User name**: Enter the user name of your account on the server; for example, `JohnDoe`.
   - **File name**: Specify the full path name of the backup file; for example, `/pub/configurations/config.txt`
   - **Password**: Enter your account password for the server. Note that this is a required field even if you are logged in as an anonymous user; in such cases, the value may be ignored by the FTP service.
6. At the “Do you want to continue [y/n]” prompt, enter `y`.
7. Wait for the configuration to be restored.

The following example shows `configDownload` run on a switch without Admin Domains:

```
switch:admin> configDownload
Protocol (scp or ftp) [ftp]: ftp
Server Name or IP Address [host]: 192.1.2.3
User Name [user]: JohnDoe
File Name [config.txt]: /pub/configurations/config.txt

*** CAUTION ***
This command is used to download a backed-up configuration for a specific switch. If using a file from a different switch, this file's configuration settings will override any current switch settings. Downloading a configuration file, which was uploaded from a different type of switch, may cause this switch to fail. A switch reboot might be required for some parameter changes to take effect.

configDownload operation may take several minutes to complete for large files.

Do you want to continue [y/n]: y
Password: ********

Activating configDownload: Switch is disabled
Updated RADIUS configuration
configDownload complete: All config parameters are downloaded.
```

switch:admin>
The following example shows `configDownload` run on a switch with Admin Domains:

```
switch:AD5:admin> configDownload
Protocol (scp or ftp) [ftp]:
Server Name or IP Address [host]: 10.1.2.3
User Name [user]: JohnDoe
File Name [config.txt]: /pub/configurations/config.txt
```

*** CAUTION ***
This command is used to download a backed-up configuration for a specific switch. If using a file from a different switch, this file's configuration settings will override any current switch settings. Downloading a configuration file, which was uploaded from a different type of switch, may cause this switch to fail. A switch reboot might be required for some parameter changes to take effect.

configDownload operation may take several minutes to complete for large files.

Do you want to continue [y/n]: y
Password: xxxxx

Activating configDownload: Switch is disabled

configDownload complete: Only zoning parameters are downloaded to ad5.

```
switch:AD5:admin>
```

8. If you disabled the switch, when the process is finished, enter the `switchEnable` command.

---

**NOTE:** Because some configuration parameters require a reboot to take effect, after you download a configuration file you must reboot to be sure that the parameters are enabled. Before the reboot, this type of parameter is listed in the configuration file, but it is not effective until after the reboot.

---

**Security considerations**

Security parameters and the switch's identity cannot be changed by `configDownload`. Parameters such as the switch's name and IP address (lines in the configuration file that begin with “boot”) are ignored. Security parameters (lines in the configuration file that begin with “sec”), such as secure mode setting and version stamp, are ignored.

For more detailed information on security, see “Configuring standard security features” on page 15.

---

**Troubleshooting configuration download**

If the configuration download fails, verify that these conditions are true:

- There was no reason to disable the switch. Note, however, that you must disable the switch for some configuration downloads. See “Configuration download without disabling a switch” on page 137.
- The host name is known to the switch.
- The host IP address can be contacted.
- You have permission on the host to perform configuration download.
- The configuration file you are trying to download exists on the host.
- The configuration file you are trying to download is a switch configuration file.
- If you selected the (default) FTP protocol, the FTP server is running on the host.
- The configuration file uses correct syntax.
- The username and password are correct.

If the switch reboots during the configuration download, issue the command again.
There may be some restrictions if you are using Admin Domains. See “Managing administrative domains” on page 143 for details.

Messages captured in the logs

Configuration download generates both RASLog and Audit log messages resulting from execution of the configDownload command.

The following messages are written to the logs:

- configDownload completed successfully ... (RASLog and Audit log)
- configUpload completed successfully ... (RASLog)
- configDownload not permitted ... (Audit log)
- configUpload not permitted ... (RASLog)
- (Warning) Downloading configuration without disabling the switch was unsuccessful. (Audit log)

Restoring configurations in a FICON environment

If the switch is operating in a FICON CUP environment, and the ASM (active=saved) bit is set on, then the switch ignores the IPL file downloaded when you restore a configuration. Table 43 describes this behavior in more detail.

Table 43  Backup and restore in a FICON CUP environment

<table>
<thead>
<tr>
<th>ASM bit</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on or off</td>
<td>configUpload</td>
<td>All the files saved in the file access facility are uploaded to the management workstation. A section in the uploaded configuration file labeled FICON_CUP is in an encoded format.</td>
</tr>
<tr>
<td>on</td>
<td>configDownload</td>
<td>Files saved on the switch that are also present in the FICON_CUP section of the configuration file are overwritten. Files in the FICON section of the configuration file that are not currently present on the switch are saved. The IPL file is not replaced, because active=saved mode is on. A warning message is displayed in the syslog to warn that the IPL file is not being overwritten.</td>
</tr>
<tr>
<td>off</td>
<td>configDownload</td>
<td>Files saved on the switch that are also present in the FICON_CUP section of the configuration file are overwritten. Files in the FICON section of the configuration file that are not currently present on the switch are saved. The IPL file is replaced, because active=saved mode is off.</td>
</tr>
</tbody>
</table>

If fmsmode is enabled in a configuration file, but is disabled on the switch, the configDownload command fails and displays an error message. This prevents undesirable conditions that could result from enabling fmsmode on a switch that does not require it.

Downloading configurations across a fabric

To save time when configuring fabric parameters and software features, you can save a configuration file from one switch and download it to other switches of the same model type, as shown in the following procedure.

Do not download a configuration file from one switch to another switch that is a different model, because it can cause the switch to fail. If you need to reset affected switches, issue the configDefault command.

**NOTE:** In some cases, the configRemoveAll root command is required for reset, in which case you should contact your system administrator.
To download a configuration file from one switch to another same model switch:

1. Configure one switch first.
2. Use the `configUpload` command to save the configuration information. See “Backing up a configuration” on page 135.
3. Run `configDefault` on each of the target switches, and then use the `configDownload` command to download the configuration file to each of the target switches. See “Restoring a configuration” on page 137.

**Configuration form**

Use Table 44 as a hard copy reference for your configuration information.

In the hardware reference manuals for the 4/256 SAN Director and DC SAN Backbone Director (short name, DC Director) there is a guide for FC port setting tables. The tables can be used to record configuration information for the various blades.

**Table 44 Configuration and connection information**

<table>
<thead>
<tr>
<th>Configuration settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td></td>
</tr>
<tr>
<td>Gateway address</td>
<td></td>
</tr>
<tr>
<td>Chassis configuration option</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management connections</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial cable tag</td>
<td></td>
</tr>
<tr>
<td>Ethernet cable tag</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain ID</td>
<td></td>
</tr>
<tr>
<td>Switch name</td>
<td></td>
</tr>
<tr>
<td>Ethernet IP address</td>
<td></td>
</tr>
<tr>
<td>Ethernet subnet mask</td>
<td></td>
</tr>
<tr>
<td>Total number of local devices (nsShow)</td>
<td></td>
</tr>
<tr>
<td>Total number of devices in fabric (nsAllShow)</td>
<td></td>
</tr>
<tr>
<td>Total number of switches in the fabric (fabricShow)</td>
<td></td>
</tr>
</tbody>
</table>
6 Managing administrative domains

This chapter provides procedures for using administrative domains (Admin Domain or AD). An Admin Domain is a logical grouping of fabric elements that defines what switches, ports, and devices you can view and modify. An Admin Domain is a filtered administrative view of the fabric.

**NOTE:** If you do not implement Admin Domains, the feature has no impact on users and you do not need to learn how to use this functionality.

Admin Domains permit access to a configured set of users. Using Admin Domains, you can partition the fabric into logical groups and allocate administration of these groups to different user accounts so that these accounts manage only the Admin Domains assigned to them and do not make changes to the rest of the fabric.

For example, you can put all the devices in a particular department in the same Admin Domain for ease of managing those devices. If you have remote sites, you could put the resources in the remote site in an Admin Domain and assign the remote site administrator to manage those resources.

You set up zones to define which devices and hosts can communicate with each other; you set up Admin Domains to define which users can manage which devices, hosts, and switches.

You can have up to 256 Admin Domains in a fabric (254 user-defined and 2 system-defined), numbered from 0 through 255. Admin Domains are designated by a name and a number. This document refers to specific Admin Domains using the format “AD\(n\)” where \(n\) is a number between 0 and 255.

**NOTE:** Do not confuse an Admin Domain number with the Domain ID of a switch. They are two different identifiers. The Admin Domain number identifies the Admin Domain and has a range of 0–255. The Domain ID identifies a switch in the fabric and has a range of 1–239.

Before using the procedures described in this chapter, you should become familiar with the Admin Domain concepts described in the following sections.

An “AD-aware switch” is a switch that runs Fabric OS 5.2.0 or later (on both CPs, if a dual CP switch) and has a valid Advanced Zoning license.

An “AD-unaware switch” is a switch that is running:

- Fabric OS 5.1.x or earlier
- Fabric OS 5.2.0 or later but does not have an Advanced Zoning license
- Fabric OS 5.2.0 or later on one CP but Fabric OS 5.1.x or earlier on the other (for dual-CP switches) and is in HA_Sync

**Figure 2** shows a fabric with two Admin Domains: AD1 and AD2.
Figure 2 Fabric with two Admin Domains

Figure 3 shows how users get a filtered view of this fabric, depending on which Admin Domain they are in. As shown in Figure 4, users can see all switches and E_Ports in the fabric, regardless of their Admin Domain; however, the switch ports and end devices are filtered based on Admin Domain membership.

Fabric Visible to AD1 User

Fabric Visible to AD2 User

Figure 3 Filtered fabric views
Admin Domain features

Admin Domains allow you to:

- Define the scope of an Admin Domain to encompass ports and devices within a switch or a fabric.
- Share resources across multiple Admin Domains. For example, you can share array ports and tape drives between multiple departments. In Figure 2, one of the storage devices is shared between AD1 and AD2.
- Have a separate zone database for each Admin Domain. See “Admin Domains, zones, and zone databases” on page 162 for more information.
- Move devices from one Admin Domain to another without traffic disruption, cable reconnects, or discontinuity in zone enforcement.
- Provide strong fault and event isolation between Admin Domains.
- Have visibility of all physical fabric resources. All switches, E_Ports, and FRUs (including blade information) are visible.
- Implement Admin Domains in a fabric with some switches running AD-unaware firmware versions (that is, firmware versions earlier than Fabric OS 5.2.0).
- Continue to run existing third-party management applications. Prior and existing versions of third party management applications continue to work with admin and user IDs.

NOTE: The Admin Domain administrator can define up to 254 ADs (AD1 – AD254) in the AD database; however, Fabric OS supports only 16 active Admin Domains running concurrently. More than sixteen active Admin Domains might cause performance degradation and unpredictable system behavior.

Requirements for Admin Domains

This section lists the requirements for implementing Admin Domains in a fabric.

- One or more switches in the fabric must be running Fabric OS 5.2.0 or later.
- The switches must have a valid Advanced Zoning license.
- The default zone mode setting must be set to No Access before you create Admin Domains (see “Implementing Admin Domains” on page 153).
- To use Admin Domains and the FC-FC Routing Service in the same fabric, the switches connecting to the FC router must be running Fabric OS 5.2.0 or later.
- If the fabric includes LSAN zones:
  - The LSAN zone names must not end with “_ADn”.
  - The LSAN zone names must not be longer than 57 characters.
- The fabric must be in the native operating mode. Admin Domains are not supported in interoperability mode.
- Gigabit Ethernet (GbE) ports cannot be members of an Admin Domain.

User-defined Administrative Domains

AD1 through AD254 are user-defined Admin Domains. These user-defined Admin Domains can be created only by a physical fabric administrator (see “Admin Domain access levels” on page 147 for more information).

In Figure 3 on page 144, AD1 and AD2 are user-defined Admin Domains.

System-defined Administrative Domains

When you install Fabric OS 6.0.0, the switch enters AD-capable mode with domains AD0 and AD255 automatically created. AD0 and AD255 are special Admin Domains. AD0 and AD255 always exist and cannot be deleted or renamed. They are reserved for use in creation and management of Admin Domains.
AD0

AD0 is a system-defined Admin Domain that, in addition to containing members you explicitly added (similar to user-defined Admin Domains), contains all online devices, switch ports, and switches that have not been assigned to any user-defined Admin Domain.

Unlike user-defined Admin Domains, AD0 has an implicit and an explicit membership list. User-defined Admin Domains have only explicit members.

- The “implicit membership list” contains all devices, switch ports, and switches that have not been assigned to any other Admin Domain.
  
  Initially, the AD0 implicit membership list contains all devices, switch ports, and switches in the fabric. This implicit membership list includes all AD-unaware switches and the devices attached to them. When you explicitly create AD1 through AD254, the devices, switch ports, and switches used to create these user-defined Admin Domains disappear from the AD0 implicit membership list.

- The “explicit membership list” contains all devices, switch ports, and switches that you explicitly add to AD0 and can be used to force device and switch sharing between AD0 and other Admin Domains. Explicit members can be added to AD0 using the `ad --add` command.

AD0 can be managed like any user-defined Admin Domain. The only difference between AD0 and user-defined Admin Domains is the implicit membership list.

The implicit members of AD0 change dynamically as the membership of other Admin Domains changes. The explicit members of AD0 are not deleted unless you explicitly remove them.

For example, if you explicitly add DeviceA to AD0 and it is not a member of any other Admin Domain, then DeviceA is both an implicit and an explicit member of AD0. If you add DeviceA to AD2, then DeviceA is deleted from the AD0 implicit membership list, but is not deleted from the AD0 explicit membership list. If you then remove DeviceA from AD2, DeviceA is added back to the AD0 implicit membership list (assuming DeviceA is not in any other Admin Domain).

When a new device is added to the fabric, it automatically becomes an implicit member of AD0 until it is explicitly added to an Admin Domain.

AD0 is useful when you create Admin Domains because you can see which devices, switch ports, and switches have not yet been assigned to any Admin Domains.

AD0 owns the root zone database (legacy zone database). During zone merge or zone update, only the root zone database is exchanged with AD-unaware switches.

AD255

AD255 is used for Admin Domain management. You can use AD255 to get an unfiltered view of the fabric and to view the hierarchical zone databases of AD0 through AD254. All Admin Domain management is done in the AD255 context.

AD255 does not have a zone database associated with it; you cannot use AD255 to perform any zoning management tasks (non-read operations such as creating or modifying zones).

Figure 5 on page 150 shows the same fabric from Figure 3, but with AD0 and AD255 shown. AD0 contains the two devices that are not in any of the user-defined Admin Domains (AD1 and AD2). AD255 encompasses the entire physical fabric.
Admin Domain access levels

Admin Domains offer a hierarchy of administrative access. To manage Admin Domains, you must be a physical fabric administrator. A “physical fabric administrator” is a user with the Admin role and access to all Admin Domains (AD0 through AD255). Only a physical fabric administrator can perform Admin Domain configuration and management.

Other administrative access is determined by your defined RBAC role and AD membership. Your role determines your access level and permission to perform an operation. Your AD membership determines the fabric resources that you can operate on.

Table 45 lists each Admin Domain user type and describes its administrative access and capabilities.

<table>
<thead>
<tr>
<th>User type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Fabric Administrators</td>
<td>User account with Admin role and with access to all Admin Domains (AD0 through AD255). Create and manage all Admin Domains. Assign other administrators or users to each Admin Domain. Only a physical fabric administrator can create other physical fabric administrators.</td>
</tr>
<tr>
<td>Administrative Domain Users</td>
<td>Can be assigned to one or more Admin Domains. Manage the resources within their Admin Domains. If their role permits, can create user accounts and assign them to Admin Domains in their list. Cannot view other Admin Domain definitions. They can view only members of their own Admin Domains.</td>
</tr>
</tbody>
</table>
Admin Domains and login

You are always logged in to an Admin Domain, and you can view and modify only the devices in that Admin Domain.

If you have access to more than one Admin Domain, one of them will have been specified as your “home Admin Domain,” the one you are automatically logged in to. If your home Admin Domain is deleted or deactivated, then by default you are logged in to the lowest numbered active Admin Domain in your Admin Domain List. The home Admin Domain, like the Admin Domain list, is a configurable property of a non-default user account. Here is some information about AD accounts:

- You can log in to only one Admin Domain at a time. You can later switch to a different Admin Domain (see “Switching to a different Admin Domain context” on page 161).
- For default accounts such as admin and user, the home Admin Domain defaults to AD0 and cannot be changed.
- The Admin Domain list for the default admin account is 0–255, which gives this account automatic access to any Admin Domain as soon as the domain is created, and makes this account a physical fabric administrator.
- The Admin Domain list for the default user account is AD0 only.
- For user-defined accounts, the home Admin Domain also defaults to AD0 but an administrator can set the home Admin Domain to any Admin Domain to which the account has been given access.
- If you are in any Admin Domain context other than AD0, the Admin Domain number is included in the system prompt displayed during your session. The following are example prompts for when you are in the AD0, AD1, and AD255 contexts, respectively:

  sw5:admin>
  sw5:AD1:admin>
  sw5:AD255:admin>

Admin Domain member types

You define an Admin Domain by identifying members of that domain. Admin Domain members can be devices, switch ports, or switches. Defining these member types is similar to defining a traditional zone member type. An Admin Domain does not require or have a new Domain ID or management IP address linked to it.

The following sections describe these member types in more detail.

Device members

Device members are defined by the device World Wide Name (WWN). A device member:

- Can be either a device port WWN or device node WWN.
- Grants view access to the device and zoning rights.
- Provides a pure virtual view. The cabling and switch port diagnostics and control is done by the physical fabric administrator.

View rights are also granted to the switch port to which the device is attached.

Port control is provided only through switch port membership and is not provided for device members. When you create an Admin Domain, the end device members do not have to be online, even though their WWNs are used in the Admin Domain definition. The physical fabric administrator performs cabling and switch port diagnostics and control.

You can share device members across multiple Admin Domains. You can also zone shared devices differently in each Admin Domain. A device WWN member does not automatically grant usage of corresponding domain,port members in the zone configuration. If you specify a device WWN member in the Admin Domain member list, zone enforcement ignores zones with the corresponding port (the port to which the device is connected) member usage.
Switch port members

Switch port members are defined by switch domain, port. A switch port member:

• Grants port control rights and zoning rights for that switch port.
• Grants view access and zoning rights to the device connected to that switch port.
• Allows you to share domain, port members across multiple Admin Domains. In each Admin Domain, you can also zone shared devices differently.
• Implicitly includes all devices connected to the specified domain, port members in the Admin Domain membership.
• Allows you to specify a range of ports as Admin Domain members. For example: \(<D, [0-15]\)>. The port range arguments are expanded and stored in the Admin Domain member list.

If a device is a member of an Admin Domain, the switch port to which the device is connected becomes an indirect member of that Admin Domain and the domain, port is removed from the AD0 implicit membership list.

**NOTE:** The domain, port members are not automatically changed when the switch Domain ID changes.

Switch members

Switch members are defined by the switch WWN or Domain ID. A switch member:

• Grants administrative control to the switch.
• Grants port control for all ports in that switch.
• Allows switch administrative operations such as switchDisable, switchEnable, reboot, and firmwareDownload.
• Does not provide zoning rights for the switch ports or devices.

To allow devices to be zoned within Admin Domains, you must specify the port members using domain, port or device WWN members.

E_Ports (E_Ports, VE_Ports, EX_Ports, and VEX_Ports) are implicitly shared across all Admin Domains. An administrator can perform port control (such as portDisable or portEnable) only if the domain, port of the E_Port is part of the Admin Domain.

**NOTE:** Only the WWN of the switch is saved in the Admin Domain. If you change the Domain ID of the switch, the Admin Domain ownership of the switch is not changed.

Admin Domains and switch WWN

Admin Domains are treated as fabrics. Because switches cannot belong to more than one fabric, switch WWNs are converted so that they appear as unique entities in different Admin Domains (fabrics). This WWN conversion is done only in the AD1 through AD254 context. AD0 and AD255 use unconverted switch WWNs. The switch WWN has the following format:

10:00:nn:nn:nn:nn:nn

In an Admin Domain context, the switch WWN is converted from NAA=1 to NAA=5 format, with the Admin Domain number added, using the following syntax:


where xx is the AdminDomain_number.

For example, if the switch WWN is:

10:00:00:60:69:e4:24:e0

then the converted WWN for that switch in AD1 would be:

50:06:06:9e:42:4e:09:01
Managing administrative domains

Figure 5 shows an unfiltered view of a fabric with two switches, three devices, and two Admin Domains. The devices are labeled with device WWNs and the switches are labeled with Domain ID and switch WWNs.

Figure 5 Fabric showing switch and device WWNs

Figure 6 shows the filtered view of the fabric as seen from AD3 and AD4. The switch WWNs are converted to the NAA=5 syntax; the device WWNs and Domain IDs remain the same.

Figure 6 Filtered fabric views showing converted switch WWNs

Admin Domain compatibility and availability

Admin Domains maintain continuity of service for Fabric OS features and operate in mixed-release fabric environments. High Availability is supported with some backward compatibility. The following sections describe the continuity features of Admin Domain usage.

Admin Domains and merging

When an E_Port comes online, the adjacent switches merge their AD databases. The receiving switch accepts an AD database from the neighboring switch only if the local AD database is empty or if the new
AD database exactly matches both the defined and effective configurations of the local AD database. If the AD database merge fails, the E_Port is segmented with “AD conflict” error code.

Compatibility

Admin Domains can be implemented in fabrics with a mix of AD-aware switches and AD-unaware switches. The following considerations apply:

- In mixed-fabric configurations, the legacy switches allow unfiltered access to the fabric and its devices; hence, these legacy switches should be managed by the physical fabric administrator.
- You must zone all ports and devices from legacy switches in the AD0 root zone database.
- If you have legacy switches in your AD-activated fabric, you must ensure that all new AD resources have enough interconnectivity so that they do not get isolated into subfabrics with a legacy subfabric interposed in the middle, as shown in Figure 7.

![Isolated subfabrics](image.png)

**Figure 7** Isolated subfabrics

Firmware upgrade and downgrade scenarios

You cannot perform a firmware downgrade to a Fabric OS version earlier than 5.2.0 if ADs are configured in the fabric. Following are special scenarios for director class products only:

- If the primary and secondary CPs are running pre-Fabric OS 5.2.0 and are in HA-Sync, and if `firmwaredownload` is used to upgrade one CP alone (using the `firmwaredownload -s` option), then that CP will run in an AD-unaware mode (AD creation operations will fail and the local switch will show up as an AD-unaware switch in the fabric).
- If the primary and secondary CPs are running Fabric OS 5.2.0 or later, and if ADs are configured, any attempt to downgrade one or both CPs to pre-Fabric OS 5.2.0 versions will fail. The Admin Domain configuration must be cleared before you can perform the downgrade (see “Deleting all user-defined Admin Domains” on page 158).

Managing Admin Domains

This section is for physical fabric administrators who are managing Admin Domains. You must be a physical fabric administrator to perform the tasks in this section.

- “Implementing Admin Domains” on page 153
- “Creating an Admin Domain” on page 153
- “Assigning a user to an Admin Domain” on page 154
- “Activating and deactivating Admin Domains” on page 155
- “Adding and removing Admin Domain members” on page 156
- “Renaming an Admin Domain” on page 157
- “Deleting an Admin Domain” on page 157
- “Deleting all user-defined Admin Domains” on page 158
- “Validating an Admin Domain member list” on page 158
Understanding the AD transaction model

You use the `ad` command to perform most of the tasks in this section. This command follows a batched-transaction model, which means that changes to the Admin Domain configuration occur in the transaction buffer.

An Admin Domain configuration can exist in several places:

- **Effective configuration**—The Admin Domain configuration that is currently in effect.
- **Defined configuration**—The Admin Domain configuration that is saved in flash memory. There might be differences between the effective configuration and the defined configuration.
- **Transaction buffer**—The Admin Domain configuration that is in the current transaction buffer and has not yet been saved or canceled.

How you end the transaction determines the disposition of the Admin Domain configuration in the transaction buffer. The following commands end the Admin Domain transaction:

- `ad --save` Saves the changes in the transaction buffer to the defined configuration in persistent storage and propagates the defined configuration to all switches in the fabric. Note that for delete and clear operations, if one or more of the deleted Admin Domains are in the effective configuration, you cannot use `--save`, but must use `--apply` instead.
- `ad --apply` Saves the changes to the defined configuration in persistent storage and enforces the defined configuration on all switches in the fabric, replacing the effective configuration.
- `ad --transabort` Aborts the transaction and clears the transaction buffer. The effective and defined configurations remain unchanged.

You can enter the `ad --transshow` command at any time to display the ID of the current Admin Domain transaction.

Detailed information about CLI syntax and options is available in the *Fabric OS Command Reference*.

Implementing Admin Domains

To begin implementing an Admin Domain structure within your SAN, you must first set the default zone mode to No Access. You must be in AD0 to change the default zone mode. You can use the `defZone --show` command to see the current default zone mode setting.

To set the default zone mode:

1. Log in to an AD-aware switch in the fabric with the appropriate RBAC role.
2. Ensure you are in the AD0 context.
   
   Use the `ad --show` command to determine the current Admin Domain and the `ad --select 0` command to switch to the AD0 context, if necessary.
3. Enter the `defZone --noAccess` command, and respond to the prompt with a `y`.
4. Enter the `cfgSave` command.

   ```
   sw5:admin> defzone --noaccess
   You are about to set the Default Zone access mode to No Access
   Do you want to set the Default Zone access mode to No Access ? (yes, y, no, n): [no] y
   
   sw5:admin> cfgsave
   You are about to save the Defined zoning configuration. This action will only save the changes on Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.
   Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y
   Updating flash ... 
   sw5:admin>
   ```
Creating an Admin Domain

To create an Admin Domain, you must specify an Admin Domain name, number, or both.

- If you create an Admin Domain using only a number, the Admin Domain name is automatically assigned to be “AD\text{n}”, where \text{n} is the number you specified.
  For example, if you specify AD number = 4, then AD name is set to “AD4”.
- If you create an Admin Domain using only a name, the Admin Domain number is automatically assigned and is the lowest available AD number, except if you specify a name in the format “AD\text{n}”, in which case the Admin Domain number is assigned to be \text{n}.
  For example, if you specify AD name = “blueAD” and the lowest available AD number is 5, then AD name is “blueAD” and AD number is 5.
  If you specify AD name = “AD15” and the lowest available AD number is 6, then AD name is “AD15” and AD number is 15. Because the specified name is in the format “AD\text{n}”, the AD number is assigned to be \text{n} and not the lowest available AD number.

The Admin Domain name cannot exceed 63 characters and can contain alphabetic and numeric characters. The only special character allowed is an underscore (_).

When you create an Admin Domain, you must specify at least one member (switch, switch port, or device). You cannot create an empty Admin Domain. For more information about these member types, see “Admin Domain member types” on page 148.

You create Admin Domains in the transaction buffer using the \text{ad} --create command. You can either save the newly created Admin Domain to a defined configuration (using \text{ad} --save) or make it the effective Admin Domain configuration directly (using \text{ad} --apply).

The following procedures describe the steps for creating Admin Domains and include examples.

To create an Admin Domain:

1. Log in as the physical fabric administrator to an AD-aware switch in the fabric.
2. Set the default zone mode to No Access, if you have not already done so.
   See “To set the default zone mode:” on page 153 for instructions.
3. Switch to the AD255 context, if you are not already in that context:
   \text{ad} --select 255

4. Enter the \text{ad} --create command using the \text{-d} option to specify device and switch port members and the \text{-s} option to specify switch members:
   \text{ad} --create \text{ad\_id} \text{-d} "\text{dev\_list}" \text{-s} "\text{switch\_list}"
   where \text{ad\_id} is the Admin Domain name or number, \text{dev\_list} is a list of device WWNs or domain,port members, and \text{switch\_list} is a list of switch WWNs or Domain IDs.

5. To end the transaction now, enter \text{ad} --save to save the Admin Domain definition or enter \text{ad} --apply to save the Admin Domain definition and directly apply the definitions to the fabric.

The following example creates Admin Domain AD1, consisting of two switches, which are designated by Domain ID and switch WWN.

sw5:AD255:admin> \text{ad} --create AD1 -s "97; 10:00:00:60:69:80:59:13"
The following example creates Admin Domain “blue\_ad,” consisting of two switch ports (designated by domain,port), one device (designated by device WWN), and two switches (designated by Domain ID and switch WWN).  

sw5:AD255:admin> \text{ad} --create blue\_ad -d "100; 5; 1,3; 21:00:00:e0:8b:05:4d:05; -s "97; 10:00:00:60:69:80:59:13"
Assigning a user to an Admin Domain

After you create an Admin Domain, you can specify one or more user accounts as the valid accounts who can use that Admin Domain. You create these user accounts using the `userConfig` command. User accounts have the following characteristics with regard to Admin Domains:

- A user account can only have a single role.
  - You can choose roles from one of the seven types of roles, either the existing user and administrator role or one of the other RBAC roles.
- You can configure a user account to have access to the physical fabric through AD255 and to a list of Admin Domains (AD0–AD254).
- You can configure a user account to have access to only a subset of your own Admin Domain list. Only a physical fabric administrator can create another physical fabric administrator user account.
- Users capable of using multiple Admin Domains, can designate one of these Admin Domains as the home Admin Domain, which is the default Admin Domain context after login.
- If you do not specify one, the home Admin Domain is the lowest valid Admin Domain in the numerically-sorted AD list.
- Users can log in to their Admin Domains and create their own Admin Domain-specific zones and zone configurations.
- Adding an Admin Domain list, home Admin Domain, and role to a user configuration is backward compatible with pre-Fabric OS 5.2.0 firmware. When you downgrade to pre-Fabric OS 5.2.0 firmware, the `userConfig` command records are interpreted using legacy logic.

To create a new user account for managing Admin Domains:

1. Connect to the switch and log in as admin.
2. Enter the `userconfig --add` command using the `-r` option to set the role, the `-a` option to provide access to Admin Domains, and the `-h` option to specify the home Admin Domain.

```
userconfig --add username -r role -h home_AD -a "AD_list"
```

where `username` is the name of the account, `role` is the user account role, `home_AD` is the home Admin Domain, and `AD_list` is the list of Admin Domains to which the user account will have access.

The following example creates new user account ad1admin with an admin role and assigns one Admin Domain, blue_ad1, to it. This example also assigns blue_ad1 as the user’s home Admin Domain.

```
sw5:admin> userconfig --add ad1admin -r admin -h blue_ad1 -a "blue_ad1"
```

The following example creates new user account ad2admin with an admin role, access to Admin Domains 1 and 2, and home Admin Domain set to 2.

```
sw5:admin> userconfig --add ad2admin -r admin -h 2 -a "1,2"
```

To assign Admin Domains to an existing user account:

1. Connect to the switch and log in as admin.
2. Enter the `userConfig --addad` command using the `-a` option to provide access to Admin Domains and the `-h` option to specify the home Admin Domain.

```
userconfig --addad username -h home_AD -a "AD_list"
```

where `username` is the name of the account, `home_AD` is the home Admin Domain, and `AD_list` is the list of Admin Domains to which the user account will have access.

The following example assigns Admin Domain green_ad2 to the existing user account ad1admin.

```
sw5:admin> userconfig --addad ad1admin -r admin -a "green_ad2"
```

To create a new physical fabric administrator user account:

1. Connect to the switch and log in as admin.
2. Enter the `userconfig --add` command using the `-r` option to set the role to admin and the `-a` option to provide access to Admin Domains 0 through 255.

```
userconfig --add username -r admin -h home_AD -a "0-255"
```

154 Managing administrative domains
where \textit{username} is the name of the account and \textit{home AD} is the home Admin Domain.

The following example creates new user account \texttt{pf_admin1} with an admin role, access to all Admin Domains (AD0 through AD255), and home Admin Domain set to 255. This user account is now a physical fabric administrator.

\begin{verbatim}
sw5:admin> userconfig --add pf_admin1 -r admin -h 255 -a "0-255"
\end{verbatim}

### Activating and deactivating Admin Domains

An Admin Domain can be in either an active or inactive state. When you create an Admin Domain, it is automatically in the active state.

If you deactivate an Admin Domain, the members assigned to the Admin Domain can no longer access their hosts or storage unless those members are part of another Admin Domain.

You cannot log in to an Admin Domain that has been deactivated. You must activate an Admin Domain before you can log in to it.

To activate an Admin Domain:

1. Connect to the switch and log in as admin.
2. Switch to the AD255 context, if you are not already in that context.

   \begin{verbatim}
   ad --select 255
   \end{verbatim}

3. Enter the \texttt{ad --activate} option. The activate option prompts for confirmation. On default, after the Admin Domain is activated, the devices specified under that AD are not able to see each other until they are zoned together.

4. To end the transaction now, enter \texttt{ad --save} to save the Admin Domain definition or enter \texttt{ad --apply} to save the Admin Domain definition and directly apply the definitions to the fabric.

The following example activates Admin Domain AD_B5.

\begin{verbatim}
sw5:AD255:admin> ad --activate AD_B5
You are about to activate a new admin domain. Do you want to activate 'AD_B5' admin domain (yes, y, no, n): [no]: y
\end{verbatim}

To deactivate an Admin Domain:

1. Connect to the switch and log in as admin.
2. Disable the zone configuration under the Admin Domain you want to deactivate.
3. Switch to the AD255 context, if you are not already in that context.

   \begin{verbatim}
   ad --select 255
   \end{verbatim}

4. Enter the \texttt{ad --deactivate} option. The \texttt{ad --deactivate} option prompts for confirmation.

5. To end the transaction now, enter \texttt{ad --save} to save the Admin Domain definition or enter \texttt{ad --apply} to save the Admin Domain definition and directly apply the definitions to the fabric.

All active user sessions associated with the Admin Domain are terminated. The deactivate option does not disable ports.

The following example deactivates Admin Domain AD_B4.

\begin{verbatim}
sw5:AD255:admin> ad --deactivate AD_B4
You are about to deactivate an AD. This operation will fail if an effective zone configuration exists in the AD
Do you want to deactivate 'AD_B5' admin domain (yes, y, no, n): [no] y
\end{verbatim}
Adding and removing Admin Domain members

Use the following procedures to add or remove members of an Admin Domain.

**NOTE:** If you remove the last member of an Admin Domain, that Admin Domain is automatically deleted.

To add members to an existing Admin Domain:

1. Connect to an AD-aware switch and log in as admin.
2. Switch to the AD255 context, if you are not already in that context.
   
   `ad --select 255`
3. Enter the `ad --add` command using the `-d` option to specify device and switch port members and the `-s` option to specify switch members:
   
   `ad --add ad_id -d "dev_list" -s "switch_list"`

   where `ad_id` is the Admin Domain name or number, `dev_list` is a list of device WWNs or `domain,port` members, and `switch_list` is a list of switch WWNs or Domain IDs.
4. To end the transaction now, enter `ad --save` to save the Admin Domain definition or enter `ad --apply` to save the Admin Domain definition and directly apply the definitions to the fabric.

The following example adds two switch ports, designated by `domain,port`, to Admin Domain AD1.

```
sw5:AD255:admin> ad --add AD1 -d "100,5; 4,1"
```

To remove members from an Admin Domain:

1. Connect to the switch and log in as admin.
2. Switch to the AD255 context, if you are not already in that context.
   
   `ad --select 255`
3. Enter the `ad --remove` command using the `-d` option to specify device and switch port members and the `-s` option to specify switch members:
   
   `ad --remove ad_id -d "dev_list" -s "switch_list"`

   where `ad_id` is the Admin Domain name or number, `dev_list` is a list of device WWNs or `domain,port` members, and `switch_list` is a list of switch WWNs or Domain IDs.

   Removing the last member element of an Admin Domain deletes the Admin Domain.
4. To end the transaction now, enter `ad --save` to save the Admin Domain definition or enter `ad --apply` to save the Admin Domain definition and directly apply the definitions to the fabric.

   The following example removes port 5 of domain 100 and port 3 of domain 1 from AD1.

```
sw5:AD255:admin> ad --remove 1 --d "100,5; 1,3"
```

The following example removes switch 100 from the membership list of AD4.

```
sw5:AD255:admin> ad --remove 4 --s "100"
```

Renaming an Admin Domain

Use this procedure if you want to change the name of an Admin Domain. You can also change auto-assigned names (ADn).

To rename an Admin Domain:

1. Connect to the switch and log in as admin.
2. Switch to the AD255 context, if you are not already in that context.
   
   `ad --select 255`
3. Enter the `ad --rename` command with the present name and the new name.
   
   `ad --rename present_name new_name`
The rename operation does not take effect if the Admin Domain you want to rename is part of the effective configuration and thus enforced.

4. To end the transaction now, enter `ad --save` to save the Admin Domain definition or enter `ad --apply` to save the Admin Domain definition and directly apply the definitions to the fabric. The Admin Domain numbers remain unchanged after the operation.

The following example changes the name of Admin Domain Eng_AD to Eng_AD2.

sw5:AD255:admin> ad --rename Eng_AD Eng_AD2

Deleting an Admin Domain

When you delete an Admin Domain its devices no longer have access to the members of the zones with which it was associated.

To delete an Admin Domain:

1. Connect to the switch and log in as admin.
2. Delete the zone database under the Admin Domain.
3. Switch to the AD255 context.
   
   ```
   ad --select 255
   ```
4. Enter the `ad --delete` command.
   
   ```
   ad --delete ad_id
   ```
   The `ad --delete` command prompts you for confirmation before triggering the deletion. The command will succeed, whether the administration domain is in an activated or deactivated state.
5. Enter the `ad --apply` command to save the Admin Domain definition and directly apply the definitions to the fabric.

The following example deletes Admin Domain AD_B3.

sw5:AD255:admin> ad --delete AD_B3
You are about to delete an AD.
The operation will fail if zone configuration exists in the AD
Do you want to delete ‘AD_B3’ admin domain (yes, y, no, n): [no] y

Deleting all user-defined Admin Domains

When you clear the Admin Domain configuration, all user-defined Admin Domains are deleted, the explicit membership list of AD0 is cleared, and all fabric resources (switches, ports, and devices) are returned to the implicit membership list of AD0.

You cannot clear the Admin Domain configuration if zone configurations exist in any of the user-defined Admin Domains.

To clear all Admin Domain definitions:

1. Clear all individual AD zone databases, in separate transactions, before proceeding with this operation.
2. Connect to the switch and log in as admin.
3. Switch to the AD255 context, if you are not already in that context.
   
   ```
   ad --select 255
   ```
4. Enter the `ad --clear` command.
   
   ```
   ad --clear
   ```
   This option prompts you for confirmation before triggering the delete of all Admin Domains.
5. Enter the `ad --apply` command to save the Admin Domain definition and directly apply the definitions to the fabric.

sw5:AD255:admin> ad --clear
You are about to delete all ADs definitions.
The operations will fail if zone configurations exists in AD1-AD254
Do you want to clear all admin domains (yes, y, no, n): [no] y
sw5:AD255:admin>
Validating an Admin Domain member list

The `ad --validate` option allows you to validate the device and switch member list and flag all resources that are from AD-unaware switches. You can use the `validate` option to list Admin Domain members from AD-unaware switches and non-existing or offline Admin Domain members.

You can use the `validate` option to identify misconfigurations of the Admin Domain. For example, in fabrics with a mix of AD-aware and AD-unaware switches, elements in the Admin Domain member list from old AD-unaware switches are not enforced.

The Admin Domain validation process is not applicable for AD0, as AD0 implicitly contains all unassigned and AD-unaware online switches and their devices.

To list the switches and devices in an AD member list:

1. Connect to the switch and log in as admin.
2. Switch to the AD255 context, if you are not already in that context.
   ```
   ad --select 255
   ```
3. Enter the `ad --validate` command.
   ```
   ad --validate ad_id -m mode
   ```

   If you do not specify any parameters, the entire AD database (transaction buffer, defined configuration, and effective configuration) is displayed.

   If you do not specify an Admin Domain, information about all existing Admin Domains is displayed.

   The `-m mode` flag can be used as follows:
   - 0 to display the Admin Domain configuration in the current transaction buffer.
   - 1 to display the Admin Domain configuration stored in the persistent memory (defined configuration).
   - 2 to display the currently enforced Admin Domain configuration (effective configuration).

   The following example validates the member list of Admin Domain 10 in the current transaction buffer.
   ```
   sw5:AD255:admin> ad --validate 10 -m 0
   ```

Using Admin Domains

This section is for users and administrators and describes how you use Admin Domains. If you are a physical fabric administrator and you want to create, modify, or otherwise manage Admin Domains, see “Managing Admin Domains” on page 152.

The Admin Domain looks like a virtual switch or fabric to a user. However, based on the user role and type (User_ID), users are presented with only their relevant AD-based views (see Figure 3 and Figure 4). Any devices and switch ports that are not defined as part of the Admin Domain are not shown and are not available to that AD user.

Each Admin Domain can also have its own zone configurations (defined and effective) with zones and aliases under them.

Using CLI commands in an AD context

The CLI command input arguments are validated against the AD member list; they do not work with input arguments that specify resources that are not members of the current Admin Domain. All commands present filtered output—showing only the members of the current Admin Domain.

For example, `switchShow` displays details for the list of AD members present in that switch.

- Since all E_Ports and EX_Ports are shared across all Admin Domains, they are shown under all Admin Domains.
- Other ports are displayed without any attribute details (with an explanation that they are not part of the current Admin Domain).

A port or device appears in CLI command output or other management tool outputs if any one of the conditions listed in Table 46 is met.
RASLog and SYSlog output is not filtered based on AD membership. See the Fabric OS Command Reference for more detailed information about command syntax and usage and to understand how existing commands behave in an AD context.

### Executing a command in a different AD context

The `ad --exec` option executes a command in a different Admin Domain. The Admin Domain must be one that you can access. This option creates a new shell with the current user_id, switches to the specified Admin Domain, performs the specified command, and exits the shell.

To execute a command in a different Admin Domain context:

1. Connect to the switch and log in.
2. Enter the `ad --exec` command, specifying the Admin Domain and the command you want to execute.
   ```
   ad --exec ad_id "command"
   ```

   The following example executes the `switchShow` command in the AD7 context.
   ```
   sw5:AD255:admin> ad --exec 7 "switchshow"
   ```

### Displaying an Admin Domain configuration

The `ad --show` option displays the membership information and zone database information of the specified Admin Domain. Note the following differences in the information displayed based on the Admin Domain:

- **AD255**: if you do not specify the AD_name or number, all information about all existing Admin Domains is displayed.
- **AD0-AD254 contexts**: the membership of the current Admin Domain is displayed.
- **AD0**: the device and switch list members are categorized into implicit and explicit member lists.

To show an Admin Domain:

1. Connect to the switch and log in as any user type.
2. Enter the `ad --show` command.
   ```
   ad --show
   ```

   If you are in the AD0 context, you can use the `-i` option to display the implicit membership list of AD0; otherwise, only the explicit membership list is displayed.
   ```
   ad --show -i
   ```

   If you are in the AD255 context, all Admin Domain configuration from the transaction buffer, defined configuration, and effective configuration is displayed, unless you use the `-m` option:
   ```
   ad --show ad_id -m mode
   ```

   where `ad_id` is the Admin Domain for which you want to display information and `mode` is one of the following:

   - 0 to display the Admin Domain configuration in the current transaction buffer.
   - 1 to display the Admin Domain configuration stored in the persistent memory (defined configuration).
   - 2 to display the currently enforced Admin Domain configuration (effective configuration).

---

<table>
<thead>
<tr>
<th>For</th>
<th>Condition</th>
</tr>
</thead>
</table>
| `domain,port` | The port is specified in the `domain,port` member list of the Admin Domain.  
                | One or more WWNs specified in the AD member list is attached to the `domain,port`. |
| **Device WWN** | The device WWN is specified in the AD WWN member list.                      
                | The device WWN is attached to one of the `domain,port` specified in the AD member list. |
The following example displays membership information about AD1.

```
sw5:AD1:admin> ad --show
Current AD Number: 1  AD Name: TheSwitches

Effective configuration:
------------------------
AD Number: 1 AD Name: TheSwitches State: Active

Switch WWN members: 50:06:06:99:00:2a:e9:01;
                      50:00:51:e0:23:36:f9:01;
                      50:06:06:98:05:be:99:01;
```

Switching to a different Admin Domain context

The `ad --select` option is used to switch between different Admin Domain contexts. This option creates a new shell with a new Admin Domain context. If the corresponding Admin Domain is not yet activated, the `select` option fails.

To switch to a new Admin Domain context:

1. Connect to the switch and log in as any user type.
2. Enter the `ad --select` command and the Admin Domain you want to switch to.
3. To leave the new Admin Domain context, exit from the shell.

You cannot switch to another Admin Domain context from within the shell created by `ad --select`. You must first exit the shell and then issue the `ad --select` command again.

The following example switches to the AD12 context. Note that the prompt changes to display the Admin Domain.

```
sw5:admin> ad --select 12
sw5:AD12:admin>
```

Performing zone validation

If you are working with zones, you should be aware of how they impact Admin Domains. Zone objects can be part of an Admin Domain. You can use the `zone --validate` command to list all zone members that are not part of the current zone enforcement table. A member might not be part of the zone enforcement table because:

- The device is offline.
- The device is online, but is connected to an AD-unaware switch.
- The device is online but is not part of the current Admin Domain.

For more information about the `zone` command and its use with Admin Domains, see the Fabric OS Command Reference.

Admin Domain interactions

The administrative domain feature provides interaction with other Fabric OS features and across third-party applications. You can manage Admin Domains with Web Tools applications and with Fabric Manager. If the current Admin Domain owns the switch, you can perform Fabric Watch operations.

Admin Domain interactions do not extend to user session tunneling across switches. A user logged into a switch can control only the local switch ports as specified in the Admin Domain.

When the fabric is in secure mode, the following applies:

- There is no support for ACL configuration under each Administrative Domain.
- ACL configuration commands are allowed only in AD0 and AD255. None of the policy configurations are validated with AD membership.
Table 47 lists some of the Fabric OS features and considerations that apply when using Admin Domains.

Table 47  Admin Domain interaction with Fabric OS features

<table>
<thead>
<tr>
<th>Fabric OS feature</th>
<th>Admin Domain interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLs</td>
<td>If no user-defined Admin Domains exist, you can run ACL configuration commands in only AD0 and AD255. If any user-defined Admin Domains exist, you can run ACL configuration commands only in AD255. You cannot use ACL configuration commands or validate ACL policy configurations against AD membership under each Admin Domain.</td>
</tr>
<tr>
<td>Advanced Performance Monitoring (APM)</td>
<td>All APM-related filter setup and statistics viewing is allowed only if the local switch is part of the current Admin Domain.</td>
</tr>
<tr>
<td>Fabric Watch</td>
<td>Fabric Watch configuration operations are allowed only if the local switch is part of the current Admin Domain.</td>
</tr>
<tr>
<td>FCR</td>
<td>You can create LSAN zones as a physical fabric administrator or as an individual AD administrator. The LSAN zone can be part of the root zone database or the AD zone database. FCR collects the LSAN zones from all ADs. If both edge fabrics have matching LSAN zones and both devices are online, FCR triggers a device import. LSAN zone enforcement in the local fabric occurs only if the AD member list contains both of the devices (local and imported device) specified in the LSAN zone. To support legacy applications, WWNs are reported based on the AD context using NAA=5. As a result, you cannot use the NAA=5 field alone in the WWN to detect an FC router.</td>
</tr>
<tr>
<td>FDMI</td>
<td>FDMI operations are allowed only in AD0 and AD255.</td>
</tr>
<tr>
<td>FICON</td>
<td>Admin Domains support FICON. However, you must perform additional steps because FICON management (CUP) requires additional physical control of the ports. You must set up the switch as a physical member of the FICON AD. DCC and SCC policies are supported only in AD0 and AD255, because ACL configurations are supported only in AD0 and AD255.</td>
</tr>
<tr>
<td>iSCSI</td>
<td>iSCSI operations are supported only in AD0.</td>
</tr>
<tr>
<td>Management applications</td>
<td>Management interfaces that access the fabric without a user’s credentials continue to get the physical fabric view. Examples include: SNMPv1, Web Tools, Fabric Manager; http access, unzoned Management Server query, FAL in-band CT requests from FAL Proxy to FAL Target, and FC-CT based management applications (such as Tivoli). Access from applications or hosts using Management Server calls can be controlled using the Management Server ACL support provided by the <code>msConfigure</code> command. Note that this is a switch-specific setting and not a fabricwide setting.</td>
</tr>
<tr>
<td>Port-Swapping and PID formats</td>
<td>Admin Domain port members are specified in <code>domain,port</code> format. Based on the PID format, a <code>domain,port</code> member indicates a slot/port in the switch. The <code>domain,port</code> member is effectively a member of that AD. If the PID format changes, all <code>domain,port</code> AD members with a port index of less than 128 are automatically converted to meet the new PID format. Port swapping has no effect on AD support as port swapping swaps only the area numbers of two ports and Admin Domains are specified using <code>domain,port</code> members. For detailed information about configuring the PID format, see “Configuring the PID format” on page 381.</td>
</tr>
<tr>
<td>RSCN</td>
<td>Admin Domains do not introduce any RSCN changes to devices or hosts.</td>
</tr>
</tbody>
</table>

Refer to the Fabric OS Command Reference for detailed information about the commands. The following sections describe Admin Domain interactions with zones, zone databases, and LSAN zones.
Admin Domains, zones, and zone databases

Each Admin Domain has its own zone database, with both defined and effective zone configurations and all related zone objects (zones, zone aliases, and zone members). Within an Admin Domain, you can configure zoning only with the devices that are present in that Admin Domain.

With a hierarchical zoning model, the name space for each Admin Domain and the root zones are separate; configurations are supported with the same zone object name appearing in the root zone database and different ADs (for example, the same zoneset name in AD1 and AD2).

Zoning operations ignore any resources not in the Admin Domain, even if they are specified in the zone. The behavior functions similarly to specifying offline devices in a zone. All zones from each Admin Domain zone configuration are enforced. The enforcement policy encompasses zones in the effective zone configuration of the root zone database and the effective zone configurations of each AD.

**NOTE:** AD zone databases do not have an enforced size limit. The zone database size is calculated by the upper limit of the AD membership definition and the sum of all the zone databases for each AD.

Admin Domains support `defzone mode of noaccess` alone. Before configuring any Admin Domain, you must set the `defzone` to `noaccess` mode. Admin Domains without effective zone configurations are presented with no access. See “Activating default zones” on page 403 for more information.

If the administrative domain feature is not active (AD1–AD254 are not configured and no explicit members are added to AD0), AD0 supports both `defzone allaccess` and `noaccess` modes.

Admin Domains introduce two types of zone database nomenclature and behavior:

- **Root zone database**—If you do not use Admin Domains, you will have only one zone database. This legacy zone database is known as the root zone database. If you create Admin Domains, you will have the root zone database, which is owned by AD0, and other zone databases, one for each user-defined Admin Domain.
  - During the zone update process, only the root zone database is sent to AD-unaware switches.
  - AD-level zone information is merged with the root zone configuration and enforced.

- **Zone databases**—The Admin Domains each have separate zone databases and zone transaction buffers. You can concurrently edit the separate zone databases. The AD zone database also has the following characteristics:
  - Each Admin Domain (AD1 through AD254) has its own zone definitions. These zone definitions include defined and effective zone configurations and all related zone objects including zones, zone aliases, and zone members. For example, you can define a zone name of test_z1 in more than one Admin Domain.
  - Each zone database has its own namespace.
  - There is no zone database linked to the physical fabric (AD255) and no support for zone database updates. In the physical fabric context (AD255), you can only view the complete hierarchical zone database, which is made up of the zone databases in AD0 through A254.
  - With AD support, zoning updates are supported selectively at each AD level. For example, a zone change in AD1 results in an update request only for the AD1 zone database.

Admin Domains and LSAN zones

LSANs under each Admin Domain are collated into a single name space and sent out to FCR phantom domains using the following format:

```
<original_LSAN_name>_<AD_num>
```

For example, a zone with name `lsan_for_linux_farm` in AD5 is internally converted to `lsan_for_linux_farm_AD005`.

LSAN zone names in AD0 are never converted for backward compatibility reasons.
The auto-converted LSAN zone names might collide with LSAN zone names in AD0 (for example, if AD0 contains lsan_for_linux_farm_AD005, this would cause a name collision). Fabric OS does not detect or report such name clash.

LSAN zone names greater than 57 characters are not converted or sent to the FCR phantom domain.

**Configuration upload and download in an AD context**

The behavior of `configUpload` and `configDownload` varies depending on the AD context and whether the switch is a member of the current Admin Domain. In the AD context, these commands include only the zone configuration of the current Admin Domain. If the switch is a member of the Admin Domain, all switch configuration parameters are saved and the zone database for that Admin Domain is also saved. Table 48 lists the sections in the configuration file and the Admin Domain contexts in which you can upload and download these sections.

The `configDefault` command does not clear zone or Admin Domain database information. This command is allowed only if the switch is a member of the current Admin Domain.

See “Maintaining configurations” on page 135 for additional information.

**Table 48  Configuration upload and download scenarios in an AD context**

<table>
<thead>
<tr>
<th>AD contexts</th>
<th>Configuration file sections</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iSCSI</td>
</tr>
<tr>
<td>AD255</td>
<td></td>
</tr>
<tr>
<td>With ADs</td>
<td>Yes</td>
</tr>
<tr>
<td>Without ADs</td>
<td>Yes</td>
</tr>
<tr>
<td>AD0</td>
<td></td>
</tr>
<tr>
<td>With ADs and switch membership</td>
<td>Yes</td>
</tr>
<tr>
<td>With ADs and without switch membership</td>
<td>Yes</td>
</tr>
<tr>
<td>Without ADs</td>
<td>Yes</td>
</tr>
<tr>
<td>AD1 – AD254</td>
<td></td>
</tr>
<tr>
<td>With switch membership</td>
<td>No</td>
</tr>
<tr>
<td>Without switch membership</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Zone databases for AD0 through AD254.
2. Only zone database for AD0.
3. Only zone database for current AD.
This chapter provides procedures for installing and maintaining firmware. Fabric OS 6.0 provides nondisruptive firmware installation.

This chapter refers to the following specific types of blades inserted into either the 4/256 SAN Director or DC SAN Backbone Director (short name, DC Director):

- FC blades or port blades contain only Fibre Channel ports: FC4-16/32/48, FC10-6, and FC8-16/32/48. FC8-32 & FC8-48 aren’t supported in 4/256 until 6.1.0.

**NOTE:** The FC8-32 and FC8-48 Director blades aren’t supported in the SAN Director 4/256 until the release of Fabric OS 6.1.x.

- AP blades contain extra processors and specialized ports: FR4-18i and FC4-16IP

**NOTE:** The FC4-16IP Director blade is not supported in the DC Director until a future Fabric OS release.

- CP blades have a control processor (CP) used to control the entire switch; they can be inserted only into slots 5 and 6 on the 4/256 SAN Director, and slots 6 and 7 on the DC Director.

- CR8 core blades provide ICL functionality between two DC Directors. they can be inserted only into slots 5 and 8 on the DC Director.

### About the firmware download process

You can download Fabric OS to a Director, which is a chassis; and to a non-chassis-based system, also referred to as a switch. The difference in the download process is that directors have two CPs and non-chassis based systems have one CP. Use the `firmwareDownload` command to download the firmware from either an FTP or SSH server by using either the FTP or SCP protocol to the switch. Or on the DC Director you can use the USB device that shipped with your unit.

The new firmware consists of multiple files in the form of RPM packages listed in a `.plist` file. The `.plist` file contains specific firmware information (time stamp, platform code, version, and so forth) and the names of packages of the firmware to be downloaded. These packages are made available periodically to add features or to remedy defects. Contact HP to obtain information about available firmware versions.

All systems maintain two partitions of nonvolatile storage areas, a primary and a secondary, to store two firmware images. The `firmwareDownload` command always loads the new image into the secondary partition. It then swaps the secondary partition to be the primary and reboots the system. After the system boots up, the new firmware is activated. `firmwareDownload` then copies the new image from the primary partition to the secondary partition.

In a dual-CP systems, the `firmwareDownload` command by default, sequentially upgrades the firmware image on both CPs using High Availability (HA) failover to prevent disruption to traffic flowing through the switch. This operation depends on HA status in the switch. If the switch does not support HA, you can still upgrade the CPs one at a time, using the `firmwareDownload -s` option. This option allows you to enable or disable autoreboot, and autocommit modes, on both Director and switch. On directors, this mode enables you to upgrade a single CP. Refer to the “Testing and restoring firmware on directors” on page 180.

If you are using a 4/256 SAN Director or DC Director with one or more AP blades: The Fabric OS automatically detects mismatches between the active CP firmware and the blade’s firmware. The auto-leveling process will automatically update the blade firmware to match the active CP. At the end of the auto-leveling process, the active CP and the blade will run the same version of the firmware.

If the firmware download process is interrupted by an unexpected reboot, the system will automatically repair and recover the secondary partition. You must wait for the recovery to complete before issuing another `firmwareDownload` command.
The command supports both non-interactive and interactive modes. If the `firmwareDownload` command is issued without any operands, or if there is any syntax error in the parameters, the command enters an interactive mode, in which you are prompted for input.

**TIP:** For each switch in your fabric, complete all firmware download changes on the current switch before issuing the `firmwareDownload` command on the next switch. This process ensures nondisruption of traffic between switches in your fabric.

To verify the `firmwareDownload` process is complete, enter the `firmwareDownloadStatus` command on the switch, verify the process is complete, then move on to the next switch.

---

**Upgrading and downgrading firmware**

*Upgrading* means installing a newer version of firmware. *Downgrading* means installing an older version of firmware.

In most cases, you will be upgrading firmware; that is, installing a newer firmware version than the one you are currently running. However, some circumstances may require installing an older version; that is, downgrading the firmware. The procedures in this section assume that you are upgrading firmware, but they work for downgrading as well, provided the old and new firmware versions are compatible. Always reference the latest *HP StorageWorks Fabric OS release notes* for updates that may exist regarding downgrades.

Using the CLI (or Web Tools), you can upgrade the firmware on one switch at a time. You can also use the optional Fabric Manager application to upgrade firmware simultaneously on multiple switches.

**Effects of firmware changes on accounts and passwords**

Table 49 describes what happens to accounts and passwords when you replace the switch firmware with a different version.

<table>
<thead>
<tr>
<th>Change</th>
<th>First time</th>
<th>Subsequent times (After upgrade, then downgrade, then upgrade)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrading</td>
<td>Default accounts and their passwords are preserved.</td>
<td>User-defined and default accounts and their passwords are preserved.</td>
</tr>
<tr>
<td>Downgrading</td>
<td>User-defined accounts are no longer valid. Default accounts and their passwords are preserved. If a default account was disabled, it is reenabled after the downgrade.</td>
<td>User-defined and default accounts and their passwords are preserved, including accounts added after the first upgrade.</td>
</tr>
</tbody>
</table>

For details on administrative domains and the firmware download, see “Managing administrative domains” on page 21 for more information. For more details on older releases of Fabric OS, see “Understanding legacy password behavior” on page 499.

For details about testing and restoring firmware, see “Testing and restoring firmware on directors” on page 180.

**Considerations for FICON CUP environments**

To prevent channel errors during nondisruptive firmware installation, the switch CUP port must be taken offline from all host systems.
Preparing for firmware downloads

Before executing a firmware download, it is recommended that you perform the tasks listed in this section. In the unlikely event of a failure or time-out, the preparation tasks that are described in this section will enable you to provide HP the information required to perform advanced troubleshooting.

It is recommended that you perform a configUpload to back up the current configuration before you download firmware to a switch. See “Backing up a configuration” on page 131 for details.

To prepare for a firmware download:

1. Read the HP StorageWorks Fabric OS 6.x release notes to determine if there are any updates related to firmware download.

2. Connect to the switch and log in as admin. Enter the firmwareShow command to verify the current version of Fabric OS. HP does not support upgrades from more than one previous release. For example, upgrading from Fabric OS 5.3.0 to 6.0 is supported, but upgrading from Fabric OS 5.2.x or a previous release directly to 6.0 is not.

   In other words, upgrading a switch from Fabric OS 5.2.x or a previous release to 6.0 is a two-step process—first upgrade to 5.3.0 and then upgrade to 6.0.

   **NOTE:** IP6 and DNS are supported by firmwareDownload in 6.0. If DNS is enabled and a server name instead of a server IP address is specified in the command line, firmwareDownload determines whether IP4 or IP6 should be used.

   To be able to mention the FTP server by name, you must enter at least one DNS server using the dnsconfig command.

3. Perform a configupload prior to the firmwaredownload. Save the config file on your FTP or SSH server.

4. (Optional) For additional support, connect the switch to a computer with a serial console cable. Ensure that all serial consoles (both CPs for directors) and all Telnet sessions are logged and included with any trouble reports.

5. Connect to the switch and log in to the switch as admin. Enter the supportSave command to retrieve all current core files prior to executing the firmware download. This helps to troubleshoot the firmware download process if a problem is encountered.

   If you are upgrading a Director, log in to both the active and standby CPs and enter the supportSave command on each CP.

   If you do not know the CP address, use the ipAddrShow command to view a list of all CP IP addresses associated with the switch.

6. (Optional) Enter the errClear command to erase all existing messages in addition to internal messages.
When checking connected switches, ensure that any older versions are supported. See the recommended version (shown in Table 50) before upgrading firmware on the switch. Go to http://www.hp.com to view end-of-life policies.

### Table 50  Recommended firmware

<table>
<thead>
<tr>
<th>Switch model</th>
<th>Earliest compatible version</th>
<th>Recommended version for interoperating with Fabric OS 6.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP StorageWorks 1 Gb Switch</td>
<td>Not supported in same fabric with 6.x switches.</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Switch 2/8 EL,</td>
<td>3.2.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Switch 2/16,</td>
<td>3.2.1b</td>
<td></td>
</tr>
<tr>
<td>MSA SAN Switch 2/8</td>
<td>3.2.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks Core Switch 2/64,</td>
<td>5.0.5c</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Director 2/128 in 3 and 4 only.</td>
<td>5.0.5f</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Switch 2/8V,</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Switch 2/16V,</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Switch 2/32,</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Director 2/128</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Director 2/128</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 4/256 SAN Director,</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 4/8 SAN Switch,</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 4/16 SAN Switch,</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 4/64 SAN Switch,</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks B-Series MP Router Blade(FR4-18i),</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 16 Port 4Gb Blade (FC4-16),</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 32 Port 4Gb Blade (FC4-32),</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 400 MP Router,</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 4/32 SAN Switch</td>
<td>5.1.1b</td>
<td></td>
</tr>
<tr>
<td>Brocade 4Gb SAN Switch for HP p-Class BladeSystem,</td>
<td>5.2.1b</td>
<td></td>
</tr>
<tr>
<td>Brocade 4Gb SAN Switch for HP c-Class BladeSystem</td>
<td>5.2.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 48 Port 4Gb Blade (FC4-48)</td>
<td>5.2.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks B-Series iSCSI Director Blade</td>
<td>5.2.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks 4/32B SAN Switch</td>
<td>5.2.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks SAN Director 2/328 SAN Switch</td>
<td>5.2.1b</td>
<td></td>
</tr>
<tr>
<td>HP StorageWorks MP Router</td>
<td>XPath OS 7.4.x</td>
<td>XPath OS 7.4.1e</td>
</tr>
<tr>
<td>Fabric Manager</td>
<td>5.2.0a</td>
<td>5.4.0a</td>
</tr>
</tbody>
</table>
Refer to the Fabric OS Compatibility section of the HP StorageWorks Fabric OS 6.x release notes, for the recommended firmware version.

If the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP cClass BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, or 400 MP Router switches are adjacent and you start firmware downloads on them at the same time, there may be traffic disruption.

To determine if you need to upgrade switches connected to the switch you are upgrading, use the following procedure on each connected switch to display firmware information and build dates.

To find switch version:
1. Connect to the switch and log in as admin.
2. Enter the `version` command.
   
   The following information is displayed:
   - **Kernel** displays the version of switch kernel operating system.
   - **Fabric OS** displays the version of switch Fabric OS.
   - **Made on** displays the build date of firmware running in switch.
   - **Flash** displays the install date of firmware stored in nonvolatile memory.
   - **BootProm** displays the version of the firmware stored in the boot PROM.

Obtaining and decompressing firmware

Firmware upgrades are available for customers on the HP website at [http://www.hp.com](http://www.hp.com).

You must decompress the firmware before you can use the `firmwareDownload` command to update the firmware on your equipment. Use the UNIX `tar` command for .tar files, the `gunzip` command for all .gz files, or a Windows unzip program for all .zip files.

When you unpack the downloaded firmware, it expands into a directory that is named according to the version of Fabric OS it contains. For example, if you download and unzip Fabric OS 6.0 zip, it expands into a directory called 6.0. When you issue the `firmwareDownload` command, there is an automatic search for the correct package file type associated with the switch. Specify only the path up to and including the 6.0 directory.

Performing `firmwareDownload` on switches

HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP cClass BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, and 400 MP Router switches also maintain primary and secondary partitions for firmware. The `firmwareDownload` command defaults to an autocommit option that automatically copies the firmware from one partition to the other.

You should not override autocommit under normal circumstances; use the default. See “Testing and restoring firmware on directors” on page 180 for details about overriding the autocommit option.

Overview of the firmware download process on switches

The following list describes the default behavior after you enter the `firmwareDownload` command (without options) on HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP cClass BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, and 400 MP Router switches:

- The Fabric OS downloads the firmware to the secondary partition.
- The system performs a high-availability reboot (haReboot). After the haReboot, the former secondary partition is the primary partition.
- The system replicates the firmware from the primary to the secondary partition.
- Software application (SA) software is upgraded only when `firmwareDownload` is issued with the SA option. Refer to the application’s manual for further information.
Installing and maintaining firmware

170 Installing and maintaining firmware

The upgrade process first downloads and then commits the firmware to the switch. While the upgrade is proceeding, you can start a session on the switch and use the `firmwareDownloadStatus` command to observe the upgrade progress if you wish.

**TIP:** After you start the process, do not enter any disruptive commands (such as reboot) that will interrupt the process. The entire firmware download and commit process takes approximately 17 minutes. If there is a problem, wait for the time-out (30 minutes for network problems). Disrupting the process can render the switch inoperable and require you to seek help from HP.

Do not disconnect the switch from power during the process because the switch could become inoperable when rebooted.

To upgrade firmware for HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP c-Class BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, and 400 MP Router:

1. Verify that the FTP or SSH server is running on the host server and that you have a user ID on that server.
2. Obtain the firmware file from the HP website at [http://www.hp.com](http://www.hp.com) and store the file on the FTP or SSH server.
3. Unpack the compressed files preserving directory structures.
   The firmware is in the form of RPM packages with names defined in a `.plist` file. The `.plist` file contains specific firmware information and the names of packages of the firmware to be downloaded.
4. Connect to the switch and log in as admin.
5. Issue the `firmwareShow` command to check the current firmware version on connected switches. Upgrade their firmware if necessary before proceeding with upgrading this switch. See “Checking connected switches” on page 168 for details.
6. Enter the `firmwareDownload` command.
7. Respond to the prompts as follows:

   - **Server Name or IP Address**: Enter the name or IP address of the FTP server, or SSH server for SCP, where the firmware file is stored; for example, 192.1.2.3. IP6 and DNS are supported by `firmwareDownload` in 5.3.0 and later. If DNS is enabled and a server name instead of a server IP address is specified in the command line, `firmwareDownload` determines whether IP4 or IP6 should be used.

   - **User name**: Enter the user name of your account on the server; for example, “JaneDoe”.

   - **File name**
     - **5.2.0 or later**: Specify the fully-qualified path name of the firmware directory, for example, `/pub/5.3.0`. Absolute path names may be specified using forward slashes (/).
     - **5.1.0 or earlier**: Specify the full path name of the firmware directory, appended by `release.plist`; for example, `/pub/5.2.0/release.plist`.

   **Note**: For 5.x switches, do not attempt to locate the `release.plist` file in the top level directory; there is a `release.plist` file for each platform, and the correct one is automatically selected.
8. At the “Do you want to continue [y/n]” prompt, enter y.
9. After the HA reboot, connect to the switch and log in again as admin.
10. If you want snapshots of the upgrade progress, use a separate session and enter the firmwareDownloadStatus command to monitor the firmware download.
11. After the firmware commit is completed, which takes several minutes, enter the firmwareShow command to display the firmware level of both partitions.

```
Stealth200E:admin> firmwareDownload
Server Name or IP Address: 192.168.126.115
User Name: userfoo
File Name: /userfoo/firmware/5.3.0
Network Protocol(1-auto-select, 2-FTP, 3-SCP) [1]: 2
Password: 
Checking system settings for firmwareDownload...
Trying address-->AF_INET IP: 192.168.126.115, flags : 2
System settings check passed.
You can run firmwareDownloadStatus to get the status of this command.

This command will cause a warm/non-disruptive boot on the switch, but will require that existing telnet or SSH sessions be restarted.

Do you want to continue [Y]: y
Firmware is being downloaded to the switch. This step may take up to 30 minutes.
```

**Downloading firmware to a Director**

You can download firmware to the HP StorageWorks 4/256 SAN Director and DC Director without disrupting the overall fabric if the two CP blades are installed and fully synchronized. Use the haShow command to verify that the CPs are synchronized prior to beginning the firmware download process. If only one CP blade is inserted or powered on, you can run firmwareDownload -s to upgrade the CP. If the CPs are not in sync, you can run firmwareDownload -s on each of the CPs to upgrade them. These operations will be disruptive. Or if the CPs are not in sync, run the haSyncStart command. If the problem persists, review “Troubleshooting firmwareDownload” on page 183. If the troubleshooting information fails to help resolve the issue, contact HP.

During the upgrade process, the Director fails over to its standby CP blade and the IP addresses for the logical switches move to that CP blade’s Ethernet port. This may cause informational ARP address reassignment messages to appear on other switches in the fabric. This is normal behavior, because the association between the IP addresses and MAC addresses has changed.

**TIP:** To successfully download firmware, you must have an active Ethernet connection on each of the CPs.
Overview of the firmware download process on directors

The following summary describes the default behavior of the `firmwareDownload` command (without options) on the 4/256 SAN Director and DC Director. After you enter the `firmwareDownload` command on the active CP blade the following actions occur:

1. The standby CP blade downloads firmware.
2. The standby CP blade reboots and comes up with the new Fabric OS.
3. The active CP blade synchronizes its state with the standby CP blade.
4. The active CP blade forces a failover and reboots to become the standby CP blade.
5. The new standby CP blade (the active CP blade before the failover) downloads firmware.
6. The new standby CP blade reboots and comes up with the new Fabric OS.
7. The new active CP blade synchronizes its state with the new standby CP blade.
8. The `firmwareCommit` command runs automatically on both CP blades.

**TIP:** After you start the process, do not enter any disruptive commands (such as reboot) that will interrupt the process. The entire firmware download and commit process takes approximately 15 minutes. If there is a problem, wait for the time-out (30 minutes for network problems). Disrupting the process can render the switch inoperable and require you to seek help from HP.

Do not disconnect the switch from power during the process because the switch could become inoperable upon reboot.

4/256 SAN Director and DC Director `firmwareDownload` procedure

There is only one logical switch address for the 4/256 SAN Director and DC Director.

**NOTE:** By default, the `firmwareDownload` command automatically upgrades both the active and standby CP on the 4/256 SAN Director. It also automatically upgrades both the active and the standby CP and all co-CPs on the CP blades. It automatically upgrades all AP blades in the 4/256 SAN Director and DC Director using auto-leveling.

To upgrade firmware on 4/256 SAN Director and DC Director (including blades):

1. Verify that the FTP or SSH server is running on the host server and that you have a user ID on that server.
2. Obtain the firmware file from the HP website at [http://www.hp.com](http://www.hp.com) and store the file on the FTP or SSH server.
3. Unpack the compressed files preserving directory structures.
   The firmware is in the form of RPM packages with names defined in a `.plist` file. The `.plist` file contains specific firmware information and the names of packages of the firmware to be downloaded.
4. Connect to the switch and log in as admin.
5. Use the `firmwareShow` command to check the current firmware version on connected switches.
   Upgrade the firmware, if necessary, before proceeding with upgrading this switch.
   See “Checking connected switches” on page 168
6. Enter the `hashow` command to confirm that the two CP blades are synchronized. In the following example, the active CP blade is CP0 and the standby CP blade is CP1:

```bash
switch:admin> hashow
Local CP (Slot 5, CP0): Active, Warm Recovered
Remote CP (Slot 6, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```
CP blades must be synchronized and running Fabric OS 4.2.0 or later to provide a nondisruptive download. If the two CP blades are not synchronized, enter the haSyncStart command to synchronize them. If the CPs still are not synchronized, contact HP.

7. Enter the firmwareDownload -s command.

8. Respond to the prompts as follows:

Server Name or IP Address
Enter the name or IP address of the FTP server, or SSH server for SCP, where the firmware file is stored; for example, 192.1.2.3. IP6 and DNS are supported by firmwareDownload in 5.3.0. If DNS is enabled and a server name instead of a server IP address is specified in the command line, firmwareDownload determines whether IP4 or IP6 should be used.

User name
Enter the user name of your account on the server; for example, “JaneDoe”.

File name
5.3.0 or later: Specify the fully qualified path name of the firmware directory, for example, /pub/5.3.0. Absolute path names may be specified using forward slashes (/).

5.2.0 or earlier: Specify the full path name of the firmware directory, appended by release.plist; for example, /pub/5.2.0/release.plist.

Note: For 4.x and 5.x switches only, do not attempt to locate the release.plist file in the top level directory; there is a release.plist file for each platform, and the correct one is automatically selected.

Network protocol
Specify the file transfer protocol used to download the firmware from the file server. Valid values are FTP and SCP. The Values are not case-sensitive. If “-p” is not specified, firmwareDownload will determine the protocol automatically by checking the config.security parameter on the switch.

Password
Enter a password. This operand can be omitted if firmware is accessible through a local directory, or if no password is required by the FTP server. This operand is required when accessing an SSH server.

9. At the “Do you want to continue [y/n]” prompt, enter y.

The firmware is downloaded to one CP blade at a time, beginning with the standby CP blade. During the process, the active CP blade fails over. After the firmware is downloaded, a firmware commit starts on both CP blades. The entire firmware download and commit process takes approximately 15 minutes.

If an AP blade is present: At the point of the failover an autoleveling process is activated. Autoleveling is triggered when the active CP detects a blade that contains a different version of the firmware, regardless of which version is older. Autoleveling downloads firmware to the AP blade, swaps partitions, reboots the blade, and copies the new firmware from the primary partition to the secondary partition. If you have multiple AP blades, they are updated simultaneously; however, the downloads can occur at different rates.
Autoleveling takes place in parallel with the firmware download being performed on the CPs, but does not impact performance. Fibre Channel traffic is not disrupted during autoleveling, but GbE traffic on AP blades may be affected.

sw77:admin> firmwaredownload
Type of Firmware (FOS, SAS, or any application) [FOS]:
Server Name or IP Address: 192.168.32.10
Network Protocol (1-auto-select, 2-FTP, 3-SCP) [1]:
User Name: userfoo
File Name: /home/userfoo/5.3.0
Password:

Verifying the input parameters ...

Verifying the system parameters for firmwaredownload... 

The following AP blades are installed in the system.

<table>
<thead>
<tr>
<th>Slot</th>
<th>Name</th>
<th>Versions</th>
<th>Traffic Disrupted</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>FC4-16IP</td>
<td>5.3.0</td>
<td>GigE</td>
</tr>
<tr>
<td>4</td>
<td>FR4-18i</td>
<td>5.3.0</td>
<td>None</td>
</tr>
<tr>
<td>10</td>
<td>FR4-18i</td>
<td>5.3.0</td>
<td>None</td>
</tr>
</tbody>
</table>

This command will upgrade both CPs and all AP blade(s) above. It will temporarily disrupt the specified traffic on the AP blade(s) when it activates the new firmware. If you want to upgrade a single CP only, please use -s option.

You can run firmwareDownloadStatus to get the status of this command.

This command will cause the active CP to reset and will require that existing telnet or SSH sessions be restarted.

Do you want to continue [Y]: y

The firmware is being downloaded to the Standby CP. It may take up to 10 minutes

Do you want to continue [Y]: y

10. Optionally, after the failover, connect to the switch, and log in again as admin. Using a separate session to connect to the switch, enter the firmwareDownloadStatus command to monitor the firmware download status.

sw77:root> firmwareDownloadstatus
[1]: Thu Jul 28 00:30:49 2005
Slot 2 : Firmware is being downloaded to the blade. It may take up to 30 minutes.

[2]: Thu Jul 28 00:30:49 2005
Slot 7 : Firmware is being downloaded to the blade. It may take up to 30 minutes.

[3]: Thu Jul 28 00:37:42 2005
Slot 2 : Firmware has been downloaded successfully to the blade.

[4]: Thu Jul 28 00:37:42 2005
Slot 7 : Firmware has been downloaded successfully to the blade.

[5]: Thu Jul 28 00:37:50 2005
Slot 2 : Blade is rebooting.

[6]: Thu Jul 28 00:37:50 2005
Slot 7 : Blade is rebooting.

[7]: Thu Jul 28 00:37:50 2005
Slot 2 : Firmware commit is started.
Step 11. Enter the `firmwareShow` command to display the new firmware versions. Following is an example of `firmwareShow` output on the 4/256 SAN Director.

```
switch:admin> firmwareShow
Slot Name  Appl  Primary/Secondary Versions  Status
-----------------------------------------------------------
2  FC4-16  FOS    5.3.0                      5.3.0
5  CP0     FOS    5.3.0 Standby *
6  CP0     FOS    5.3.0 Active
7  FC4-16  FOS    5.3.0                      5.3.0

* Local CP
```

Note: If Local CP and Remote CP have different versions of firmware, please retry `firmwareDownload` command.

**Director restrictions for downgrading**

Note the following restrictions:

- **4/256 SAN Director with one or more FR4-18i blades:** If you are running 5.1.0 firmware, then you cannot downgrade to earlier versions without removing the blades.
- **4/256 SAN Director with one or more FC4-48 or FC4-16IP blades:** If you are running Fabric OS 5.2.0, then you cannot downgrade to earlier versions without removing the blades.
- Do not remove blades until the EX_Ports are removed first. The `firmwareDownload` command will indicate when the blades are safe to remove.
- **4/256 SAN Director with one or more FC10-6 blades:** If you are running Fabric OS 6.0.0b, then you cannot downgrade to earlier versions without removing the blades.
- **4/256 SAN Director with one or more FC8-16 blades:** If you are running Fabric OS 6.0.0b, then you cannot downgrade to earlier versions without removing the blade.
- **DC Director with FC8-16/32/48 blades:** If you are running Fabric 6.0.0b, then you cannot downgrade to earlier versions of Fabric OS as they are not supported on this Director.
The DC Director supports a firmware download from the USB device attached to the active CP.

**NOTE:** The USB device ships with the DC Director only.

Before the USB device can be accessed by the `firmwaredownload` command, it must be enabled and mounted as a file system. The firmware images to be downloaded must be stored under the `/firmware` directory in the USB file system. Multiple images can be stored under this directory. There is a `firmwarekey` directory where the public key signed firmware is stored.

When the `firmwaredownload` command line option, `-U` (upper case), is specified, the `firmwaredownload` command will download the specified firmware image from the USB device. When specifying a path to a firmware image in the USB device, you can only specify the relative path to `/firmware` or the absolute path.

To enable USB:
1. Log in to the switch using an account assigned to the admin role.
2. Type the following command:
   ```
   usbstorage -e
   ```

To view the USB file system:
1. Log in to the switch using an account assigned to the admin role.
2. Type the `usbstorage -l` command:
   ```
   admin>usbstorage -l
   /usb/usbstorage/brocade/firmware/6.0.0/
   /usb/usbstorage/brocade/firmwarekey/pubkey.pem
   ```

To download the 6.0 image using the relative path:
1. Log in to the switch as admin.
2. Type the `firmwaredownload` command with the `-U` operand:
   ```
   admin>firmwaredownload -U 6.0
   ```

To download the 6.0 image using the absolute path:
1. Log in to the switch as admin.
2. Type the `firmwaredownload` command with the `-U` operand:
   ```
   admin>firmwaredownload -U /usb/usbstorage/brocade/firmware/6.0
   ```
FIPS Support

Federal information processing standards (FIPS) specify the security standards needed to satisfy a cryptographic module utilized within a security system for protecting sensitive information in the computer and telecommunication systems. For more information about FIPS, refer to “Configuring advanced security features” on page 17.

The 6.0 firmware is digitally signed using the OpenSSL utility to provide FIPS support. In order to use the digitally signed software, you need to configure the switch to enable Signed Firmwaredownload. If it is not enabled then the firmware download process will ignore the firmware signature and work as before.

If Signed Firmwaredownload is enabled, and if the validation succeeds, the firmware download process will proceed normally. If the firmware is not signed or if the signature validation fails, firmwaredownload will fail. So when you are downgrading to 5.3.0, you need to disable Signed Firmwaredownload.

To enable or disable FIPS, refer to “Configuring advanced security features” on page 17.

Public and private key management

For signed firmware, we use RSA with 1024-bit length key pair. The Fabric OS requires a private key to sign the firmware files. During firmwareDownload, the process requires the public key to validate the signatures of the firmware files. So the public key needs to be stored on the switch beforehand. The following describes how the key pairs will be managed for the current and future releases.

The switch manufacturer generates one private and public key pair. These key pairs are stored in the privatekey.pem and pubkey.pem files, respectively. The private key file is used to sign the firmware files. The public key file is packaged in an RPM-package as part of the firmware, and will be downloaded to the switch. After it is downloaded, it can be used to validate the firmware to be downloaded next time.

The public key file on the switch contains only one public key. It is only able to validate firmware signed using one corresponding private key. If the private key changes in the future releases, you change the public key on the switch by one of the following method:

a. By using firmwareDownload. If the public key file on the switch has not been modified after it is installed, when a new firmware is downloaded, firmwareDownload always replaces the public key file on the switch with what is in the new firmware. This allows you to have planned firmware key changes.

b. By using the firmwarekey command. This command retrieves a specified public key file from a specific server location and replaces the one on the switch.

c. Refer to the latest Fabric OS release notes for information regarding firmware versions and their corresponding public key files

If the public key file has been modified using the firmwarekey command, firmwareDownload will not replace this file in the subsequent downloads because it thinks the change is intentional. The user will need to use the firmwarekey command for subsequent updates of this file.

A different firmware key pair will be created for digitally signed firmware releases. The private key file for the digitally signed firmware releases will be used to sign released firmware, and the public key file will be packaged inside these digitally signed firmware releases.

NOTE: If FIPS is enabled, all logins should be done through SSH or direct serial and the transfer protocol should be SCP.

To update the firmwarekey:
1. Log in to the switch as admin.
2. Type the firmwarekeyupdate command.
3. Respond to the prompts as follows:

   Server Name | Enter the name or IP address of the FTP server, or SSH server for SCP, where the firmwarekey file is stored; for example, 192.1.2.3.
   Download from USB | Optional: -U (upper case) Specify this option if you want to download from the USB device attached to the active CP.
   Network protocol | Specify the file transfer protocol used to download the firmware from the file server. Valid values are FTP and SCP. The Values are not case-sensitive. If “-p” is not specified, firmwarekeyupdate will determine the protocol automatically by checking the config.security parameter on the switch.
   User name | Enter the user name of your account on the server; for example, “JaneDoe”. 
   File name | Specify the full qualified path name of the firmware directory, for example, /pub/firmwarekey/pubkey.pem,12345. Absolute path names may be specified using forward slashes (/).
   Password | Enter a password. This operand can be omitted if firmware is accessible through USB or if no password is required by the FTP server. This operand is required when accessing an SSH server.

The **firmwareDownload** command

As mentioned previously, the public key file will need to be packaged, installed, and run on your switch before downloading a signed firmware.

When **firmwareDownload** installs a firmware file, it needs to validate the signature of the file. Different scenarios are handled as follows:

   a. If a firmware file does not have a signature, how it is handled depends on the “signed_firmware” parameter on the switch. If it is enabled, **firmwareDownload** will fail. Otherwise, **firmwareDownload** will display a warning message and proceed normally. So when downgrading to a non-FIPS compliant firmware, the “signed_firmware” flag needs to be disabled.
   b. If the firmware file has a signature but the validation fails, **firmwareDownload** will fail. This means the firmware is not from HP or its content has been modified.
   c. If the firmware file has a signature and the validation succeeds, **firmwareDownload** will proceed normally.

DMM, and Third Party Application images will not be signed.

To configure the switch for signed firmware:

1. Log in to the switch as admin.
2. Type the `configure` command.
3. Respond to the prompts as follows:

   System Service or SSL attributes | Default is no; press Enter to select default setting.
   snmp attributes | Default is no; press Enter to select default setting.
   rpcd attributes | Default is no; press Enter to select default setting.
   cfgload attributes | Select Yes. The following questions are displayed:
   Webtools attributes | Default is no; press Enter to select default setting.
   System | Default is no; press Enter to select default setting.
Power-on firmware checksum test

FIPS requires the checksums of the executables and libraries on the filesystem to be validated before Fabric OS modules are launched. This is to make sure these files have not been changed after they are installed.

When firmware RPM packages are installed during firmwareDownload, the MD5 checksums of the firmware files are stored in the RPM database on the filesystem. This will go through all of the files in the RPM database. Every file compares its current checksum with the checksum that is in the RPM database. If they are different, the command will tell you.

Because the validation may take up to a few minutes, it will not be performed during hot code load. It is only performed after a cold reboot of the switch.

For more information on FIPS, see “Configuring advanced security features” on page 17.

Testing and restoring firmware on switches

Typically, users downgrade firmware after briefly evaluating a newer (or older) version and then restore the original version of the firmware. Testing a new version of firmware in this manner ensures that you do not replace existing firmware because the evaluated version occupies only one partition on the switch.

TIP: When you evaluate new firmware, make sure you disabled all features that are not supported by the original firmware before restoring to the original version.

To test a different firmware version on a switch:

1. Verify that the FTP or SSH server is running on the host server and that you have a user ID on that server.
2. Obtain the firmware file from the HP website at http://www.hp.com and store the file on the FTP or SSH server.
3. Unpack the compressed files preserving directory structures.
   The firmware is in the form of RPM packages with names defined in a .plist file, that contains specific firmware information and the names of packages of the firmware to be downloaded.
4. Connect to the switch and log in as admin.
5. Enter the firmwareShow command to view the current firmware.
6. Enter the firmwareDownload -s command to update the firmware and respond to the prompts as follows:
   switch:admin> firmwareDownload -s
   Type of Firmware (FOS, SAS, or any application) [FOS]:
   Server Name or IP Address: 192.168.32.10
   Network Protocol (1-auto-select, 2-FTP, 3-SCP) [1]:
   User Name: userfoo
   File Name: /home/userfoo/5.3.0
   Password: 
   Do Auto-Commit after Reboot [Y]: n
   Reboot system after download [N]: y
   Firmware is being downloaded to the switch. This step may take up to 30 minutes.
   Checking system settings for firmwareDownload...

   The switch will perform a reboot and come up with the new firmware to be tested. Your current switch session will automatically disconnect.

7. Connect to the switch, log in as admin, and enter the firmwareShow command to confirm that the primary partition of the switch contains the new firmware.
   You are now ready to evaluate the new version of firmware.
8. Commit the firmware.
   a. Enter the `firmwareCommit` command to update the secondary partition with new firmware. Note that it takes several minutes to complete the commit operation.
   b. Enter the `firmwareShow` command to confirm both partitions on the switch contain the new firmware.

   **IMPORTANT:** Stop! If you have completed step 8, then you have committed the firmware on the switch and you have completed the firmware download procedure. To restore the original firmware, refer to step 9 (should be performed after step 6).

9. Restore the firmware.
   a. Enter the `firmwareRestore` command. The switch will reboot and come up with the original firmware again.
      A `firmwareCommit` will automatically begin to copy the original firmware from the primary partition to the secondary partition. At the end of the firmware commit process, both partitions will have the original firmware. Note that it takes several minutes to complete the commit operation.
   b. Wait five minutes to ensure that all processes have completed and the switch is fully up and operational.
   c. Log in to the switch. Enter the `firmwareShow` command and verify that both partitions on the switch have the original firmware.

**Testing and restoring firmware on directors**

This procedure enables you to perform a firmware download on each CP and verify that the procedure was successful before committing to the new firmware. The old firmware is saved in the secondary partition of each CP until you enter the `firmwareCommit` command. If you decide to back out of the installation prior to the `firmwareCommit`, you can enter the `firmwareRestore` command to restore the former active Fabric OS firmware image.

The `firmwareRestore` command can only run if autocommit was disabled during the `firmwareDownload`.

**NOTE:** HP recommends that, under normal operating conditions, you maintain the same firmware version on both CPs, and on both partitions of each CP. This procedure enables you to evaluate firmware before you commit. As a standard practice, you should not run mixed firmware levels on CPs.

To test a different firmware version in a Director:

1. Connect to the HP logical switch IP address.
2. Enter the `ipAddrShow` command and note the address of CP0 and CP1.
3. Enter the `haShow` command and note which CP is active and which CP is standby. Verify that both CPs are in sync.
   CP blades must be synchronized and running Fabric OS 4.4.0 or later to provide a nondisruptive download. If the two CP blades are not synchronized, enter the `haSyncStart` command to synchronize them. If the CPs still are not synchronized, contact HP.
4. Enter the `firmwareShow` command and confirm that the current firmware on both partitions on both CPs is listed as expected.
5. Exit the session.
6. Update the firmware on the standby CP:
   a. Connect to the switch and log in as admin to the standby CP.
   b. Enter the `firmwareDownload -s` command and respond to the prompts.
      At this point, the firmware should download to the standby CP only. When it has completed the
download to that CP, reboot it. The current switch session will be disconnected.

7. Fail over to the standby CP.
   a. Connect to the switch on the active CP.
   b. Enter the `haShow` command to verify that HA synchronization is complete. It will take a minute or
two for the standby CP to reboot and synchronize with the active CP.

   **IMPORTANT:** If the CPs do not achieve synchronization, stop here; log in to the standby CP, and enter the
   `firmwareRestore` command to restore the original firmware.

   c. Enter the `firmwareShow` command to confirm that the primary partition of the standby CP
   contains the new firmware.
   d. Enter the `haFailover` command. The active CP will reboot and the current switch session will be
disconnected.

   **If an AP blade is present:** At the point of the failover an autoleveling process is activated. See,
   “4/256 SAN Director and DC Director firmwareDownload procedure” on page 172 for details
   about autoleveling.

8. Verify the failover:
   a. Connect to the switch on the active CP, which is the former standby CP.
   b. Enter the `haShow` command to verify that the HA synchronization is complete. It will take a minute or
two for the standby CP, which is the old active CP, to reboot and synchronize with the active CP.

   **NOTE:** If the CPs fail to synchronize, you can still proceed because the version being tested is
already present on the active CP, and subsequent steps will ensure that the standby CP is updated to
the same version as the active CP.

   c. Confirm the evaluation version of firmware is now running on the active CP by entering the
   `firmwareShow` command.

9. Update firmware on the standby CP:
   a. Connect to the switch on the standby CP, which is the old active CP.
   b. Enter the `firmwareDownload -s` command and respond to the prompts.
      At this point the firmware should download to the standby CP only and reboot it. The current switch
session will be disconnected.
   c. Wait one minute for the standby CP to reboot, and then connect to the switch and log in as admin.
   d. Enter the `firmwareShow` command to confirm that both primary partitions now have the test drive
firmware in place.
      You are now ready to evaluate the new version of firmware.

   **IMPORTANT:** Stop! If you want to restore the firmware, stop here and skip ahead to step 12;
otherwise, continue to step 10 to commit the firmware on both CPs, which completes the firmware
download.

10. Perform a commit on the standby CP.
    From the current switch session on the standby CP, enter the `firmwareCommit` command to update
the secondary partition with new firmware. It takes several minutes to complete the commit operation.
Do no do anything on the switch while this operation is in process.
11. Perform a commit on the active CP.
   a. From the current switch session on the active CP, enter the `firmwareShow` command and confirm
      that only the active CP secondary partition contains the old firmware.
   b. Enter the `firmwareCommit` command to update the secondary partition with the new firmware. It
      takes several minutes to complete the commit operation. Do not do anything on the switch while this
      operation is in process.
   c. Upon completion of the `firmwareCommit` command, type the `firmwareShow` command to
      confirm both partitions on both CPs contain the new firmware.
   d. Enter the `haShow` command to confirm that the HA state is in sync.

**IMPORTANT:** Stop! If you have completed step 11, then you have committed the firmware on both
CPs and you have completed the firmware download procedure. The following step 12 through
step 14 describe how to restore the original firmware, and should be performed after step 5.

12. Restore the firmware on the standby CP.
    In the current switch session for the standby CP, enter the `firmwareRestore` command. The standby
    CP will reboot and the current switch session will end. Both partitions will have the same Fabric OS
    after several minutes.

13. Perform `haFailover` on the active CP.
    a. In the current switch session for the active CP, enter the `haShow` command to verify that HA
       synchronization is complete. It will take a minute or two for the standby CP to reboot and
       synchronize with the active CP.
    b. Enter the `haFailover` command. The active CP will reboot and the current switch session will end.
       The switch is now running the original firmware.

14. Restore firmware on the “new” standby CP.
    a. Wait one minute and connect to the switch on the new standby CP, which is the old active CP.
    b. Enter the `firmwareRestore` command. The standby CP will reboot and the current switch session
       will end. Both partitions will have the same Fabric OS after several minutes.
    c. Wait five minutes and log in to the switch. Enter the `firmwareShow` command and verify that all
       partitions have the original firmware.

If an AP blade is present: Blade partitions always contain the same version of the firmware on
both partitions (it does not keep two copies). The firmware is stored on the blade’s compact flash
card and is always synchronized with the active CP’s firmware. Thus, if you restore the active CP
firmware, the blade firmware is automatically downloaded (auto-leveled) to become consistent with
the new CP firmware (the blade firmware is basically restored).

Your system is now restored to the original partitions on both CPs. Make sure that servers using the
fabric can access their storage devices.

If you want to upgrade a Director with only one CP in it, follow the procedures in “Testing and restoring
firmware on switches” on page 179. Note, however, that upgrading a Director with only one CP will be
disruptive to switch traffic.
Validating firmwareDownload

Validate the firmware download by running the following commands: `firmwareShow`, `firmwareDownloadStatus`, `nsShow`, `nsAllShow`, and `fabricShow`.

![NOTE: When you prepared for the firmware download earlier, you issued either the `supportShow` or `supportSave` command. Although you can issue the command again and compare the output from before and after, it may take up to 30 minutes for the command to execute. To save time, it is recommended that you use the commands listed below, which are all subsets of the `supportSave` output.

All of the connected servers, storage, and switches should be present in the output of these commands. If there is a discrepancy, it is possible that a device or switch cannot connect to the fabric and further troubleshooting is necessary.

- `firmwareShow`
  Displays the current firmware level on the switch. For directors, this command displays the firmware loaded on both partitions (primary and secondary) for both CPs and AP blades. HP recommends that you maintain the same firmware level on both partitions of each CP within the Director.

- `firmwareDownloadStatus`
  Displays an event log that records the progress and status of events during the firmwareDownload. The event log is created by the current `firmwareDownload` command and is kept until another `firmwareDownload` command is issued. There is a timestamp associated with each event. When downloading Fabric OS, the event logs in the two CPs are synchronized. This command can be run from either CP.

- `nsShow`
  Displays all devices directly connected to the switch that have logged into the name server. Make sure the number of attached devices after the firmware download is exactly the same as the number of attached devices prior to the firmware download.

- `nsAllShow`
  Displays all connected devices to a fabric. Make sure the number of attached devices after the firmware download is exactly the same as the number of attached devices prior to the firmware download.

- `fabricShow`
  Displays all switches in a fabric. Make sure the number of switches in the fabric after the firmware download is exactly the same as the number of attached devices prior to the firmware download.

You cannot perform a firmware downgrade from Fabric OS 5.2.0 or later if administrative domains are configured in the fabric. See “Managing administrative domains” on page 21 for details.

When the primary and secondary CPs in a 4/256 SAN Director are running pre-Fabric OS 5.2.0 and are in HA-Sync, and if firmware is downloaded to upgrade only one CP (using the `firmwareDownload –s` option), then that CP will run in an AD-unaware mode (AD creation operations will fail and the local switch will appear as an AD-unaware switch in the fabric).

If primary and secondary CPs are running Fabric OS 5.2.0 or later and if ADs are configured, any attempt to downgrade one or both CPs to a pre-Fabric OS 5.1.0 version will fail.

See “Troubleshooting firmwareDownload” on page 183 for exception cases and associated error messages generated from the preinstallation check.
Troubleshooting **firmwareDownload**

Starting in Fabric OS 5.2.0 a network diagnostic script and preinstallation check was added as a part of the firmwareDownload procedure. The script and preinstallation check performs troubleshooting and automatically checks for any blocking conditions. However, you should follow these best practices for firmware download before you start the procedure:

- Keep all session logs.
- Enter the `supportSave` or the `supportShow` command **before and after** entering the `firmwareDownload` command.
- If a problem persists, package together all of the information (the Telnet session logs and serial console logs, output from the `supportSave` command) for your switch support provider. Make sure you identify what information was gathered before and after issuing the `firmwareDownload` command.

If the firmware download fails, see the Fabric OS Message Reference for details about error messages. Also see, “Considerations for downgrading firmware to Fabric OS 5.3.0 or earlier” on page 184.

If a firmware download fails in a Director, the `firmwareDownload` command synchronizes the firmware on the two partitions of each CP by starting a firmware commit operation. Wait at least 10 minutes for this commit operation to complete before attempting another firmware download.

If the firmware download fails in a Director, the CPs may end up with different versions of firmware and are unable to achieve HA synchronization. In such cases, issue the `firmwareDownload -s` command on the standby CP; the single mode (`-s`) option upgrades the firmware on the standby CP to match the firmware version running on the active CP. Then re-issue the `firmwareDownload` command to download the desired firmware version to both CPs. For example, if CP0 is running 5.2.0 on the primary and secondary partitions, and CP1 is running 5.0.1 on the primary and secondary partition, then synchronize them by issuing the `firmwareDownload -s` command.

See the Fabric OS Message Reference for detailed information about .plist-related error messages.

For more information on any of the commands in the Recommended Action section, see the Fabric OS Command Reference.

---

**NOTE:** Some of the messages include error codes (as shown in the example below). These error codes are for internal use only and you can disregard them.

**Example:**

Port configuration with EX ports enabled along with trunking for port(s) 63, use the `portcfgexport`, `portcfgvexport`, and `portcfgtrunkport` commands to remedy this. Verify blade is ENABLED. (error 3).

**Considerations for downgrading firmware to Fabric OS 5.3.0 or earlier**

To avoid failure of a firmware downgrade, verify your fabric does not have any of the following conditions:

- If an FC10-6 blade is powered on in the chassis, do not remove the blade until the `firmwareDownload` command indicates that it can be removed. Removing the blades before some related features are removed is not supported.
- If an FC8-16/32/48 blade is present, power-off and remove the blade prior to downgrading the firmware.
- If there are any IP6 addresses configured, for example, switch IP address, syslog IP addresses, or RADIUS server, remove the IP6 addresses. The `firmwareDownload` command will display any IP6 addresses.
- If more than 3000 LSAN zones are configured, reduce the number of LSAN zones.
- If default IP Filter policies are not active on the switch, make the default policies active before downgrading.
- If the switch is configured with PEAP/MSCHAPv2 for RADIUS authentication, use `aaaConfig` to remove the entry.
- If QOS or FIPS is enabled, disable these features prior to downgrading the firmware.
If LDAP is configured on the switch, delete the LDAP configuration.

Preinstallation messages

The messages in this section are displayed if an exception case is encountered during firmware download from Fabric OS 5.2.0. The example earlier shows feature-related messages that you may see if you were downgrading from 5.2.0 to 5.1.0:

The following items need to be addressed before downloading the specified firmware:

- Port mirror connections detected. Please use portmirror --delete to remove these mirror connections.
- AD feature is in use. Please clear it using the ad --clear command.
- Port configuration with EX ports enabled along with trunking for port(s) 58, use the portcfgexport, portcfgvexport, and/or portcfgtrunkport commands to disable the port configuration. Verify that the blade is ENABLED. (error 3)

This example shows hardware-related messages for the same downgrade example:

director:admin> firmwaredownload
Type of Firmware (FOS, SAS, or any application) [FOS]:
Server Name or IP Address: 192.168.32.10
Network Protocol (1-auto-select, 2-FTP, 3-SCP) [1]:
User Name: userfoo
File Name: /home/userfoo/dist/5.3.0
Password:
Verifying the input parameters ...
Checking system settings for firmwaredownload...

The following items need to be addressed before downloading the specified firmware:

- AP BLADE type 24 is inserted. Please use slotshow to find out which slot it is in and remove it.
- SW BLADE type 36 is inserted. Please use slotshow to find out which slot it is in and remove it.
Firmwaredownload command failed.

director:admin>

Message

AP Blade type 24 is inserted. Please use slotshow to find out which slot it is in and remove it.

Probable cause and recommended action

The firmware download operation was attempting to download Fabric OS 5.0.0 with one or more FR4-18i port blades (blade ID 24) in the system. FR4-18i port blades are not supported on firmware 5.0.0 or earlier, so the firmware download operation is aborted.

Use the slotShow command to display which slot the FR4-18i port blade is in, and physically remove the blade(s) from the chassis. Retry the firmware download operation.

Message

AP Blade type 31 is inserted. Please use slotshow to find out which slot it is in and remove it.

Probable cause and recommended action

The firmware download operation was attempting to downgrade a system to Fabric OS 5.1.0 or earlier with one or more FC4-16IP port blades (blade ID 31) in the system. FC4-16IP port blades are not supported on firmware 5.1.0 or earlier, so the firmware download operation failed.
Use the slotShow command to display which slot the FC4-16IP port blade is in. Physically remove the blade(s) from the chassis, or use the micro-switch to turn the blade off. Retry the firmware download operation.

**Message**

AP Blade type 33 is inserted. Please use slotshow to find out which slot it is in and remove it.

Cannot downgrade due to the presence of **AP BLADE type 33**. Remove or power off these blades before proceeding.

**Probable cause and recommended action**

The firmware download operation was attempting to download Fabric OS 5.0.0 with one or more FR4-18i port blades (blade ID 33) in the system. FR4-18i port blades are not supported on firmware 5.0.0 or earlier, so the firmware download operation is aborted.

Use the slotShow command to display which slot the FR4-18i port blade is in, and physically remove the blade(s) from the chassis. Retry the firmware download operation.

**Message**

SW Blade type 36 is inserted. Please use slotshow to find out which slot it is in and remove it.

**Probable cause and recommended action**

The firmware download operation was attempting to downgrade a system to Fabric OS 5.1.0 or earlier with one or more FC4-48 port blades (blade ID 36) in the system. FC4-48 port blades are not supported on firmware 5.1.0 or earlier, so the firmware download operation failed.

Use the slotShow command to display which slot the FC4-48 port blade is in. Physically remove the blade(s) from the chassis, or use the micro-switch to turn the blade off. Retry the firmware download operation.

**Message**

SW Blade type 37 is inserted. Please use slotshow to find out which slot it is in and remove it.

**Probable cause and recommended action**

The firmware download operation was attempting to downgrade a system to Fabric OS 5.3.0 or earlier with one or more FC8-16 port blades (blade ID 37) in the system. FC8-16 port blades are not supported on firmware 5.3.0 or earlier, so the firmware download operation failed.

Use the slotShow command to display which slot the FC8-16 port blade is in. Physically remove the blade(s) from the chassis, or use the micro-switch to turn the blade off. Retry the firmware download operation.

**Message**

SW Blade type 39 is inserted. Please use slotshow to find out which slot it is in and remove it.

**Probable cause and recommended action**

The firmware download operation was attempting to downgrade a system to Fabric OS 5.2.0 or earlier with one or more FC10-6 port blades (blade ID 39) in the system. FC10-6 port blades are not supported on firmware 5.2.0 or earlier, so the firmware download operation failed.

Use the slotShow command to display which slot the FC10-6 port blade is in. Physically remove the blade(s) from the chassis, or use the micro-switch to turn the blade off. Retry the firmware download operation.
Message

SW Blade type 51 is inserted. Please use slotshow to find out which slot it is in and remove it.

Probable cause and recommended action

The firmware download operation was attempting to downgrade a system to Fabric OS 5.3.0 or earlier with one or more FC8-48 port blades (blade ID 51) in the system. FC8-48 port blades are not supported on firmware 5.3.0 or earlier, so the firmware download operation failed.

Use the slotShow command to display which slot the FC8-48 port blade is in. Physically remove the blade(s) from the chassis, or use the micro-switch to turn the blade off. Retry the firmware download operation.

Message

SW Blade type 55 is inserted. Please use slotshow to find out which slot it is in and remove it.

Probable cause and recommended action

The firmware download operation was attempting to downgrade a system to Fabric OS 5.3.0 or earlier with one or more FC8-32 port blades (blade ID 55) in the system. FC8-32 port blades are not supported on firmware 5.3.0 or earlier, so the firmware download operation failed.

Use the slotShow command to display which slot the FC8-32 port blade is in. Physically remove the blade(s) from the chassis, or use the micro-switch to turn the blade off. Retry the firmware download operation.

Message

Only platform options 1 and 5 are supported by version 6.0. Use chassisconfig to reset the option before downloading the firmware.

Probable cause and recommended action

The firmware download operation was attempting to upgrade a system to Fabric OS 6.0. The chassisConfig option was set to 2, 3 or 4, which are not supported in 6.0, so the firmware download operation was aborted.

Execute the chassisConfig command with a supported option (1 or 5 for 4/256 SAN Director; and 5 for 4/256 SAN Director and DC Director on 6.0), and then retry the firmware download operation.

The supported options are:

option 1 One 128-port switch with the following configuration:
FC2-16 (blade ID 4), FC4-16 (blade ID 17) on slots 1–4 and 7–10;
CP2 (blade ID 5), CP4 (blade ID 16) on slots 5–6

option 5 One 384-port switch with the following configuration:
FC4-16 (blade ID 17), FC4-32 (blade ID 18) FR4-18i (Blade ID 24), FR4-18i (blade ID 31, (blade ID 33), 36, FC10-6 (blade ID 39) on slots 1–4 and 7–10;
CP4 (blade ID 16) on slots 5–6

Message

Cannot downgrade to 5.1.0 because Device Based routing policy is not supported by 5.1.0. Use aptPolicy to change the routing policy before proceeding.

Probable cause and recommended action

The firmware download operation was attempting to upgrade a system to Fabric OS 5.1.0 with device-based routing policy selected. Device-based routing policy is not supported in firmware 5.1.0 or later, so the firmware download operation was aborted.
Disable the switch and change the routing policy selection to one of the following supported selections on firmware 5.1.0 using the aptPolicy command, and then retry the firmware download operation. The supported selections are:

**policy 1** Port-based routing policy

With this policy, the path chosen for an incoming frame is based on:
1. Incoming port on which the frame was received
2. Destination domain for the frame

The chosen path remains the same if the dynamic load sharing (DLS) feature is not enabled. If DLS is enabled, then a different path may be chosen on a fabric event. Refer to the dlsSet command for the definition of a fabric event.

This policy may provide better ISL utilization when there is little or no oversubscription of the ISLs.

**NOTE:** Static routes are supported only with this policy.

**policy 3** Exchange-based routing policy

With this policy, the path chosen for an incoming frame is based on:
1. Incoming port on which the frame was received
2. FC address of the Source ID (SID) for this frame
3. FC address of the Destination ID (DID) for this frame
4. FC Originator Exchange ID (OXID) for this frame

This policy allows for optimal utilization of the available paths as I/O traffic between different (SID, DID, OXID) pairs can use different paths. All frames received on an incoming port with the same (SID, DID, OXID) parameters takes the same path unless there is a fabric event. Refer to the dlsSet command for the definition of a fabric event.

This policy does not support static routes. DLS always is enabled and the DLS setting cannot change with this policy.

**Message**

Cannot downgrade due to the presence of broadcast zone(s). Remove or disable them before proceeding.

**Probable cause and recommended action**

If the switch is running 5.3.0 or higher, and a “broadcast zone” is configured, the user will not be allowed to downgrade the switch to 5.2.0 or earlier, as a broadcast zone gets a special meaning in 5.3.0, but it will be treated as regular zone in 5.2.0 or earlier.

Use the zoneRemove command to remove the zone or zoneDelete command to delete the zone.

**Message**

Cannot downgrade due to the presence of IP6 addresses on the switch. Please reconfigure these addresses before proceeding. (Firmwaredownload will tell the user which addresses are configured with IP6 and commands used for remedy.).

**Probable cause and recommended action**

If switch is running 5.3.0 or higher, and if there are any IP6 addresses configured, e.g. switch IP address, syslog IP addresses, radius server, etc. the user will not be allowed to downgrade to a version that does not support IP6.

Use the ipaddrset command to change the IP6 addresses to IP4 addresses.
Message
Cannot downgrade due to LSAN count is set to 3000, please disable it before proceeding.

Probable cause and recommended action
If a switch is running 5.3.0 or higher and the LSAN count is at 3000, then you will not be allowed to downgrade to 5.2.0 or earlier.
Use the fcrlsanmatrix command to disable the LSAN.

Message
Cannot downgrade due to LSAN zone binding is enabled. Please disable it before proceeding.

Probable cause and recommended action
If switch is running 5.3.0 or higher, and if LSAN zone binding is enabled, the user will not be allowed to downgrade to 5.2.0 or earlier.
Use the fcrlsanmatrix command to disable the LSAN.

Message
Cannot downgrade to 5.2.0 or lower due to GE port(s) has MTU size configured between 1261 to 1499 bytes. Please use portcfg command to reconfigure the mtu size and try again.

Probable cause and recommended action
If a GE port has its MTU size configured between 1261 to 1499 bytes, you will not be allowed to downgrade to 5.2.0 or earlier.
Use the portcfg command to reconfigure the MTU size and try again.

Message
Cannot downgrade to 5.2.0 or lower because ge port(s) has IPSec and Fastwrite enabled. Please use portcfg command to disable Fastwrite and try again.

Probable cause and recommended action
If a GE port has IPSec and Fastwrite enabled, the user will not be allowed to downgrade to 5.2.0 or earlier.
Use the portcfg command to disable IPSec and try again.

Message
Cannot downgrade to 5.2.0 or lower because GE port(s) has DHCP enabled. Please use portcfg command to disable it and try again.

Probable cause and recommended action
If a GE port has DHCP enabled, you will not be allowed to downgrade to 5.2.0 or earlier.
Use the portcfg command to disable it and try again.

Message
Cannot downgrade due to presence of port mirror connections. Use portmirror --delete to remove these mirror connections before proceeding.

Probable cause and recommended action
The firmware download operation was attempting to downgrade a system to Fabric OS 5.1.0 or earlier with Port Mirroring enabled. Port Mirroring is not supported on firmware 5.1.0 or earlier, so the firmware download operation failed.
Remove the mirror connections using the portMirror --delete command. Retry the firmware download operation.
Message

Cannot upgrade directly to 5.3.0. Upgrade your switch to 5.1 or 5.2 first before upgrading to the requested version.

Probable cause and recommended action

If the switch is running 5.0.0 or earlier, you will not be allowed to upgrade directly to 5.3.0 because of the “two-version” rule.

Upgrade your switch to Fabric OS version 5.1.0 or 5.2.0 before upgrading to 5.3.0

Message

Cannot upgrade due to the presence of an existing zone named “broadcast”. Rename this zone before proceeding.

Probable cause and recommended action

If the switch is running 5.1.0 or 5.2.0, and if an existing zone is named “broadcast”, the user will not be allowed to upgrade the switch to the 5.3.0 firmware, as broadcast zone gets a special meaning in 5.3.0.

Use the zoneDelete command to delete the zone.

Message

The command failed due to presence of long-distance ports in LS mode. Please remove these settings before proceeding.

Probable cause and recommended action

The firmware download operation was attempting to downgrade a system to Fabric OS 5.0.0 or earlier with long-distance ports in LS mode. Long-distance ports in LS mode is not supported in firmware 5.0.0 or earlier, so the firmware download operation failed.

Change the long distance port setting to a supported distance setting using the portCfgLongDistance command and then retry the firmware download operation. The supported settings are:

L0 Specify L0 to configure the port to be a regular switch port. A total of 20 full-size frame buffers are reserved for data traffic, regardless of the port’s operating speed; therefore, the maximum supported link distance is 10 km, 5 km, or 2.5 km for the port at speeds of 1 Gbps, 2 Gbps, or 4 Gbps respectively.

L0.5 Specify L0.5 (portCfgShow displays the two-letter code as LM) long distance to support a long distance link of up to 25 km. A total of 12, 25, or 50 full-size frame buffers are reserved for data traffic for the port at speeds of 1 Gbps, 2 Gbps, or 4 Gbps respectively.

L1 Specify L1 long distance to support a long distance link up to 50 km. A total of 25, 50, or 100 full-size frame buffers are reserved for data traffic for the port at speeds of 1 Gbps, 2 Gbps, or 4 Gbps respectively.

L2 Specify L2 long distance to support a long distance link up to 100 km. A total of 50, 100, or 200 full-size frame buffers are reserved for data traffic for the port at speeds of 1 Gbps, 2 Gbps, or 4 Gbps respectively.

LE Specify LE mode is used for E_Ports for distances beyond 5 Km and up to 10 Km. A total of 5, 10, or 20 full-size frame buffers are reserved for port speeds of 1 Gbps, 2 Gbps, or 4 Gbps, respectively. LE does not require an Extended Fabrics license.

LD Specify LD for automatic long-distance configuration. The buffer credits for the given E_Port are automatically configured, based on the actual link distance. Up to a total of 250 full-size frame buffers are reserved, depending upon the distance measured during E_Port initialization. If the desired distance is provided, it is used as the upper limit to the measured distance. For Bloom1-based systems, the number of frame buffers is limited to 63.

LS Specify LS mode to configure a long-distance link with a fixed buffer allocation. Up to a total of 250 full-size frame buffers are reserved for data traffic, depending on the desired distance value provided with the portCfgLongDistance command. For Bloom1-based systems, the number of frame buffers is limited to 63.
Message

The command failed due to the current zone size is not supported by the new firmware. Reduce the size of the configuration before proceeding.

Probable cause and recommended action

The firmware download operation was attempting to downgrade a system to Fabric OS 5.1.0 or earlier and the current zone size is not supported by the firmware version to be downloaded, so the firmware download operation failed.

Reduce the zone database size to 256 KB. Verify that the zone size is below the 256 KB limit using the cfgSize command. Retry the firmware download operation.

Message

Default IP Filter policies are not active on the switch. Please make the default IP4 filter policies active before downgrading.

Probable cause and recommended action

If switch is running 5.3.0 or higher, and if any of the user created IP Filter policies are active, the user will not be allowed to downgrade to 5.2.0 or lower.

Blade troubleshooting tips

Typically, issues detected during firmware download to AP blades do not require recovery actions on your part. However, if any of the following events occur, perform the appropriate following action:

• The blade is faulty (issue slotShow to confirm).
  If the blade is faulty, enter the slotPowerOff and slotPowerOn commands for the blade. If the blade still appears to be faulty, remove it and re-insert it into the chassis.

• The blade is stuck in the “LOADING” state (issue slotShow to confirm).
  If the blade remains in the loading state for a significant period of time, the firmware download will time out. Remove the blade and re-insert it. When it boots up, autoleveling will be triggered and the firmware download will be attempted again.

If you experience frequent failovers between CPs that have different versions of firmware, then you may notice multiple blade firmware downloads and a longer startup time.
8 Configuring Directors

This chapter provides procedures specific to HP StorageWorks Director models.

Changing a Director’s name

HP recommends that you customize the enterprise-class platform name for each platform. Some system logs identify devices by platform names; if you assign meaningful platform names, logs are more useful.

To change the platform name:

1. Connect to the switch and log in using an account assigned to the admin role.
2. Enter the `chassisName` command using the following syntax:
   ```
   switch:admin> chassisName "newname"
   ```
   where `newname` is the new name for the enterprise-class platform.
   
   Enterprise-class platform names can be from 1 to 15 characters long, must begin with a letter, and can contain letters, numbers, or the underscore character. It is not necessary to use the quotation marks.
3. Record the new platform name for future reference.

Identifying ports

Because Directors contain interchangeable port blades, their procedures differ from those for fixed-port switches. For example, fixed-port models identify ports by `domain, port number`, while Director models identify ports by `slot/port number`.

The HP StorageWorks 4/256 Director integrates 10 slots that contain control processor, port, and application (AP) blades:

- Slot numbers 5 and 6 contain control processor blades (CPs).
- Slot numbers 1 through 4 and 7 through 10 contain port and AP blades.

The HP StorageWorks DC SAN Backbone Director (short name, DC Director) integrates 12 slots that contain control processor, core, port, and AP blades:

- Slot numbers 6 and 7 contain control processor blades (CPs).
- Slot numbers 5 and 8 contain core blades.
- Slot numbers 1 through 4 and 9 through 12 contain port and AP blades.

**NOTE:** CPs contain communication ports for system management, and are used for low-level, chassis-wide tasks. In the 4/256 Director, CPs are used for intra-chassis switching.

Core blades are used for intra-chassis switching as well as interconnecting two DC Director chassis.

Port blades are used for host, storage, and interswitch connections.

AP blades are used for Fibre Channel Application Services and Routing Services, iSCSI bridging, FCIP, and storage virtualization.

On each port blade, a particular port must be represented by both slot number and port number.

When you have port blades with different port counts in the same Director (for example, 16-port blades and 32-port blades, or 16-port blades and 18-port blades with 16 FC ports and 2 GbE ports, or 16-port and 48-port blades), the area IDs no longer match the port numbers.
Director port numbering schemes

Table 51 lists the port numbering schemes for the 4/256 Director and DC Director.

### Table 51 Port numbering schemes for the 4/256 Director and DC Director

<table>
<thead>
<tr>
<th>Port blades</th>
<th>Numbering scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC2-16</td>
<td></td>
</tr>
<tr>
<td>FC4-16</td>
<td></td>
</tr>
<tr>
<td>FC8-16</td>
<td>Ports are numbered from 0 through 15 from bottom to top.</td>
</tr>
<tr>
<td>FC4-32</td>
<td>Ports are numbered from 0 through 15 from bottom to top on the left set of ports and 16 through 31 from bottom to top on the right set of ports.</td>
</tr>
<tr>
<td>FC8-32</td>
<td></td>
</tr>
<tr>
<td>FC4-48</td>
<td>Ports are numbered from 0 through 23 from bottom to top on the left set of ports and 24 through 47 from bottom to top on the right set of ports.</td>
</tr>
<tr>
<td>FC8-48</td>
<td></td>
</tr>
<tr>
<td>FC10-6</td>
<td>Ports are numbered from 0 through 5 from bottom to top.</td>
</tr>
<tr>
<td>FC4-16IP</td>
<td>Fibre Channel ports are numbered from 0 through 7 from bottom to top. There are also eight GbE ports (numbered ge0 – ge7, from bottom to top). Going from bottom to top, the eight FC ports appear on the bottom, followed by the eight GbE ports at the top.</td>
</tr>
<tr>
<td>FR4-18i</td>
<td>Ports are numbered from 0 through 15 from bottom to top. There are also two GbE ports (numbered ge0-ge1, from bottom to top). Going from bottom to top, the two GbE ports appear on the bottom of the blade followed by sixteen FC ports.</td>
</tr>
</tbody>
</table>

The following sections tell how to identify ports on 4/256 Director and DC Director models, and how to identify ports for zoning commands.

### By slot and port number

The port number is a number assigned to an external port to give it a unique identifier in a switch.

To select a specific port in the 4/256 Director and DC Director models, you must identify both the slot number and the port number using the format `slot number/port number`. No spaces are allowed between the slot number, the slash (/), and the port number.

The following example shows how to enable port 4 on a blade in slot 2:

```
switch:admin> portenable 2/4
```

### By port area ID

The relationship between the port number and area ID depends upon the PID format used in the fabric. When Core PID format is in effect, the area ID for port 0 is 0, for port 1 is 1, and so forth.

For 32-port blades (FC4-32, FC8-32), the numbering is contiguous up to port 15; from port 16, the numbering is still contiguous, but starts with 128. For example, port 15 in slot 1 has a port number and area ID of 15; port 16 has a port number and area ID of 128; port 17 has a port number and area ID of 129.

For 48-port blades (FC4-48, FC8-48), the numbering is the same as for 32-port blades for the first 32 ports on the blade. For ports 32 through 47, area IDs are not unique and port index should be used instead of area ID.

If you perform a port swap operation, the port number and area ID no longer match. On 48-port blades, port swapping is supported only on ports 0–15.

To determine the area ID of a particular port, enter the `switchShow` command. This command displays all ports on the current (logical) switch and their corresponding area IDs.

### By index

With the introduction of 48-port blades, indexing was introduced. Unique area IDs are possible up to 255 areas, but beyond that there needed to be some way to ensure uniqueness.
A number of fabric-wide databases supported by Fabric OS (including ZoneDB, the ACL DDC, and Admin Domain) allow a port to be designated by the use of a “D,P” (domain,port) notation. While the “P” component appears to be the port number, in up to 255 ports it is actually the area assigned to that port.

If the PID format is changed from Extended-edge to Core, the “P” value for ports 0-127 also changes. If two ports are changed using the **portSwap** command, their respective areas and “P” values are exchanged.

For ports that are numbered above 255, the “P” value is actually a logical index. The first 256 ports continue to have an index value equal to the area_ID assigned to the port. If a switch is using Core PID format, and no port swapping has been done, the port Index value for all ports is the same as the physical port numbers. Using **portswap** on a pair of ports will exchange those ports’ area_ID and index values. **Portswap** is not supported for ports above 256.

**Table 52** shows the area ID and index mapping for core PID assignment. Note that up to 255 areas, the area_ID mapping to the index is one-to-one. Beyond this, the index is similar but not exact, and in some instances the area ID is shared among multiple ports.

This table provides the area_ID/Index assignment for the maximum number of ports (used by the FC4-48 and FC8-48 blades). If your blade does not have the maximum number of ports, use the lower sections of the table to determine the area_ID and index.

<table>
<thead>
<tr>
<th>Port on blade</th>
<th>Slot 1Idx/area</th>
<th>Slot 2Idx/area</th>
<th>Slot 3Idx/area</th>
<th>Slot 4Idx/area</th>
<th>Slot 7Idx/area</th>
<th>Slot 8Idx/area</th>
<th>Slot 9Idx/area</th>
<th>Slot 10Idx/area</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>270/134</td>
<td>286/150</td>
<td>302/166</td>
<td>318/182</td>
<td>334/198</td>
<td>350/214</td>
<td>366/230</td>
<td>382/246</td>
</tr>
<tr>
<td>45</td>
<td>269/133</td>
<td>285/149</td>
<td>301/165</td>
<td>317/181</td>
<td>333/197</td>
<td>349/213</td>
<td>365/229</td>
<td>381/245</td>
</tr>
<tr>
<td>44</td>
<td>268/132</td>
<td>284/148</td>
<td>300/164</td>
<td>316/180</td>
<td>332/196</td>
<td>348/212</td>
<td>364/228</td>
<td>380/244</td>
</tr>
<tr>
<td>43</td>
<td>267/131</td>
<td>283/147</td>
<td>299/163</td>
<td>315/179</td>
<td>331/195</td>
<td>347/211</td>
<td>363/227</td>
<td>379/243</td>
</tr>
<tr>
<td>42</td>
<td>266/130</td>
<td>282/146</td>
<td>298/162</td>
<td>314/178</td>
<td>330/194</td>
<td>346/210</td>
<td>362/226</td>
<td>378/242</td>
</tr>
<tr>
<td>40</td>
<td>264/128</td>
<td>280/144</td>
<td>296/160</td>
<td>312/176</td>
<td>328/192</td>
<td>344/208</td>
<td>360/224</td>
<td>376/240</td>
</tr>
<tr>
<td>39</td>
<td>263/143</td>
<td>279/159</td>
<td>295/175</td>
<td>311/191</td>
<td>327/207</td>
<td>343/223</td>
<td>359/239</td>
<td>375/255</td>
</tr>
<tr>
<td>38</td>
<td>262/142</td>
<td>278/158</td>
<td>294/174</td>
<td>310/190</td>
<td>326/206</td>
<td>342/222</td>
<td>358/238</td>
<td>374/254</td>
</tr>
<tr>
<td>37</td>
<td>261/141</td>
<td>277/157</td>
<td>293/173</td>
<td>309/189</td>
<td>325/205</td>
<td>341/221</td>
<td>357/237</td>
<td>373/253</td>
</tr>
<tr>
<td>34</td>
<td>258/138</td>
<td>274/154</td>
<td>290/170</td>
<td>306/186</td>
<td>322/202</td>
<td>338/218</td>
<td>354/234</td>
<td>370/250</td>
</tr>
<tr>
<td>33</td>
<td>257/137</td>
<td>273/153</td>
<td>289/169</td>
<td>305/185</td>
<td>321/201</td>
<td>337/217</td>
<td>353/233</td>
<td>369/249</td>
</tr>
<tr>
<td>31</td>
<td>255/135</td>
<td>271/151</td>
<td>287/175</td>
<td>191/191</td>
<td>207/207</td>
<td>223/223</td>
<td>239/239</td>
<td>255/255</td>
</tr>
<tr>
<td>30</td>
<td>254/134</td>
<td>268/150</td>
<td>286/174</td>
<td>190/190</td>
<td>206/206</td>
<td>222/222</td>
<td>238/238</td>
<td>254/254</td>
</tr>
<tr>
<td>29</td>
<td>253/133</td>
<td>267/157</td>
<td>173/173</td>
<td>189/189</td>
<td>205/205</td>
<td>221/221</td>
<td>237/237</td>
<td>253/253</td>
</tr>
<tr>
<td>28</td>
<td>252/132</td>
<td>266/156</td>
<td>172/172</td>
<td>188/188</td>
<td>204/204</td>
<td>220/220</td>
<td>236/236</td>
<td>252/252</td>
</tr>
<tr>
<td>25</td>
<td>249/133</td>
<td>153/153</td>
<td>169/169</td>
<td>185/185</td>
<td>201/201</td>
<td>217/217</td>
<td>233/233</td>
<td>249/249</td>
</tr>
</tbody>
</table>
Basic blade management

The following sections provide procedures for powering a port blade off and on and for disabling and enabling a port blade.

Powering port blades off and on

All blades are powered on by default when the switch chassis is powered on. Blades cannot be powered off when POST or AP initialization is in progress.

**NOTE:** In the DC Director, the core blades in slots 5 and 8 cannot be powered off with the CLI interface. Manual intervention is required.
To power off a port blade:
1. Connect to the switch and log in as admin.
2. Enter the slotPowerOff command with the slot number of the port blade you want to power off.

```
switch:admin> slotpoweroff 3
Slot 3 is being powered off
switch:admin>
```

To provide power to a port blade:
1. Connect to the switch and log in as admin.
2. Enter the slotPowerOn command with the slot number of the port blade you want to power on.

```
switch:admin> slotpoweron 3
Powering on slot 3
switch:admin>
```

Disabling and enabling port blades

Port blades are enabled by default. In some cases, you will need to disable a port blade to perform diagnostics. When diagnostics are executed manually (from the Fabric OS command line), many commands require the port blade to be disabled. This ensures that diagnostic activity does not interfere with normal fabric traffic.

To disable a port blade:
1. Connect to the switch and log in as admin.
2. Enter the bladeDisable command with the slot number of the port blade you want to disable.

```
switch:admin> bladedisable 3
Slot 3 is being disabled
```

To enable a port blade:
1. Connect to the switch and log in as admin.
2. Enter the bladeEnable command with the slot number of the port blade you want to enable.

```
switch:admin> bladeenable 3
Slot 3 is being enabled
```

FR4-18i blade exceptions

You may wish to persistently disable FR4-18i blade ports that are not configured so they cannot join the fabric when the following scenarios apply:

- The FR4-18i blade ships with FOS 6.0.0b pre-installed. If this blade is inserted into a chassis running a version of FOS that is different than the revision level currently on the blade, the blade firmware will be upgraded or downgraded to match the firmware revision on the chassis.
- You have inserted the FR4-18i blade into a slot that was previously empty or contained an FC4-48, FC4-32, FC8-48, FC8-32, FC4-16, FC10-6, or FC4-16IP.
- You have turned on the power of the chassis and the FR4-18i blade in that slot was not active prior to the power-on.

If the FR4-18i blade is operational and the Director is rebooted, then after the successful bootup of the system the blade continues operations using the previous configurations.

If a previously configured FR4-18i blade is removed and another or the same FR4-18i blade is inserted into the same slot, then the ports use the previous configuration and come up enabled.

If a previously-configured FR4-18i blade is removed and an FC4-48, FC4-32, FC4-16, FC8-48, FC8-32, FC8-16, or FC10-6 blade is plugged in, then—other than the port’s EX_Port configuration—all the remaining port configurations previously applied to the FR4-18i FC_Ports can be used. The EX_Port configuration on those ports is disabled before the FC4 or FC8 port blade becomes operational. When a blade is present in the slot, then any requested port configuration is validated against the blade’s capabilities before accepting the request.
To summarize:

- When an FC4-16, FC4-32, FC8-16, FC8-32, FC10-6, or FC4-16IP blade is replaced by an FR4-18i blade, the FC configuration of the previously configured FC_Ports continues to be used, and all FC_Ports on the FR4-18i blade are persistently disabled.
- When an FR4-18i blade is replaced by an FC4-16, FC4-32, FC8-16, FC8-32, or FC10-6 blade, then the EX_Port configuration is removed from any ports that were configured as EX_Ports (equivalent to disabling the EX_Port configuration using the `portCfgEXPort` command). All remaining port configurations are retained.

**FC4-48 and FC8-48 blade exceptions**

The FC4-48 blade is compatible only with the CP4 processor blade, FC4-16/32 port blade, FR4-18i, and FC4-16IP iSCSI blade.

Because the area IDs are shared with different port IDs, the FC4-48 and FC8-48 blades support only F, G and E_Ports. They do not support FL_Ports.

Port swapping on an FC4-48 or FC8-48 is supported only on ports 0–15. For the FC4-32 and FC8-32 blades, port swapping is supported on all 32 ports. This means that if you replace a 32-port blade where a port has been swapped on ports 16–31 with a 48-port blade, the 48-port blade faults. To correct this, reinsert the 32-port blade and issue `portSwap` to restore the original area IDs to ports 16–31.

**Conserving power**

To conserve power and ensure that more critical components are the least affected by a power fluctuation, you can power off components in a specified order, using the `powerOffListSet` command.

The available power is compared to the power demand to determine if there is enough power to operate. If there is less power available than the demand, the power-off list is processed until there is enough power for operation. By default, the processing proceeds from slot 1 to the last slot in the chassis. As power becomes available, slots are powered up in the reverse order.

---

**NOTE:** Some FRUs in the chassis may use significant power, yet cannot be powered off through software. For example, a missing blower FRU may change the power computation enough to affect how many slots can be powered up.

The `powerOffListShow` command displays the power off order.
Blade terminology and compatibility

Before configuring a chassis, familiarize yourself with the Director CP blade and port blade nomenclature, as well as the port blade compatibilities. Often in procedures, only the abbreviated names for CP and port blades are used (for example, the FC4-16 blade). Table 53 includes CP and port blade abbreviations and descriptions.

Table 53  Director terminology and abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Abbreviation</th>
<th>Blade ID (slotshow)</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/256 Director control processor blade</td>
<td>CP4</td>
<td>16</td>
<td>The third generation CP blade provided with the 4/256 Director. This CP supports 1, 2, 4, and 10 Gbps port speeds, as well as 16, 32, and 48-port blades.</td>
</tr>
<tr>
<td>DC Director control processor blade</td>
<td>CP8</td>
<td>50</td>
<td>The CP blade provided with the DC Director. This CP supports 1, 2, 4, 8, and 10 Gbps port speeds, as well as 16, 32, and 48-port blades.</td>
</tr>
<tr>
<td>DC Director core blade</td>
<td>CR8</td>
<td>52</td>
<td>A 16-port blade that provides 8 Gbps connectivity between port blades in the DC Director chassis.</td>
</tr>
<tr>
<td>16-port 2-Gbps port blade</td>
<td>FC2-16</td>
<td>4</td>
<td>The second generation Director 16-port blade supporting 1 and 2 Gbps port speeds. This port blade is compatible only with the 4/256 Director CP blades.</td>
</tr>
<tr>
<td>16-port 4-Gbps port blade</td>
<td>FC4-16</td>
<td>17</td>
<td>The third generation Director 16-port blade supporting 1, 2, and 4 Gbps port speeds. This port blade is compatible only with the 4/256 Director CP blades.</td>
</tr>
<tr>
<td>32-port 4-Gbps port blade</td>
<td>FC4-32</td>
<td>18</td>
<td>A 32-port Director port blade supporting 1, 2, and 4 Gbps port speeds. This port blade is compatible only with the 4/256 Director CP blades.</td>
</tr>
<tr>
<td>48-port 4-Gbps port blade</td>
<td>FC4-48</td>
<td>36</td>
<td>A 48-port Director port blade supporting 1, 2, and 4 Gbps port speeds in chassis mode 5 with port and exchange-based routing. This port blade is compatible only with the 4/256 Director CP blades. FC4-48 blades do not support FL_Ports.</td>
</tr>
<tr>
<td>16-port 8-Gbps port blade</td>
<td>FC8-16</td>
<td>21</td>
<td>A 16-port Director port blade supporting 1, 2, 4, and 8 Gbps port speeds.</td>
</tr>
<tr>
<td>32-port 8-Gbps port blade</td>
<td>FC8-32</td>
<td>55</td>
<td>A 32-port Director port blade supporting 1, 2, 4, and 8 Gbps port speeds. This port blade is compatible only with the DC Director CP blades.</td>
</tr>
<tr>
<td>48-port 8-Gbps port blade</td>
<td>FC8-48</td>
<td>51</td>
<td>A 48-port Director port blade supporting 1, 2, 4, and 8 Gbps port speeds. FC8-48 blades support only F_Ports and E_Ports; FL_Ports are not supported. This port blade is compatible only with the DC Director CP blades. FC8-48 blades do not support FL_Ports.</td>
</tr>
<tr>
<td>6-port 10-Gbps port blade</td>
<td>FC10-6</td>
<td>39</td>
<td>A 6-port Director port blade supporting 10 Gbps port speed. Blade provides 10-Gbps ISLs. This port blade is compatible only with the 4/256 Director CP blades (using chassis configuration option 5) and the DC Director CP blades.</td>
</tr>
<tr>
<td>Fibre Channel Router blade</td>
<td>FR4-18i</td>
<td>24</td>
<td>A 16-port Fibre Channel routing and FCIP blade that also has 2 GbE ports and is compatible only with the 4/256 Director (using chassis configuration option 5) and the DC Director CP blades.</td>
</tr>
<tr>
<td>iSCSI Bridge blade</td>
<td>FC4-16IP</td>
<td>31</td>
<td>An iSCSI bridge blade that enables bridging of iSCSI hosts to Fibre Channel fabrics. It has 8 Fibre Channel optical SFP ports and 8 GbE copper RJ-45 ports. This blade is currently compatible with the 4/256 Director CP blades (using chassis configuration option 5).</td>
</tr>
</tbody>
</table>

CP blades

The 4/256 Director supports the CP4 blade. The DC Director supports the CP8 blade. Mixed CP blades are not supported on a single chassis, except during specific upgrade procedures detailed in the HP StorageWorks SAN Director hardware reference manual. CP4 and CP8 blades cannot be mixed in the same chassis under any circumstances. HP recommends that each Director have only one
type of CP blade installed and that each CP (primary and secondary partition) maintains the same firmware version.

Core blades

The DC Director supports two CR8 core blades. This blade is used for intra-chassis switching as well as ICL connectivity to another DC Director chassis.

The 4/256 Director does not support core blades.

Port blade compatibility

Table 54 identifies which port blades are supported for each Director.

Table 54 Port blades supported by each Director

<table>
<thead>
<tr>
<th>Port blades</th>
<th>Director 4/256 Director (CP4)</th>
<th>DC Director</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC2-16</td>
<td>Supported¹</td>
<td>N/A</td>
</tr>
<tr>
<td>FC4-16</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>FC4-32</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>FC4-48</td>
<td>Supported</td>
<td>N/A</td>
</tr>
<tr>
<td>FC8-16</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>FC8-32</td>
<td>N/A</td>
<td>Supported</td>
</tr>
<tr>
<td>FC8-48</td>
<td>N/A</td>
<td>Supported</td>
</tr>
<tr>
<td>FC10-6</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>FC4-16IP</td>
<td>Supported</td>
<td>N/A</td>
</tr>
</tbody>
</table>

¹. Can coexist only with FC4-16 blades.

Setting chassis configuration options for the 4/256 Director

The chassisConfig command allows you to display or set the chassis configuration on the 4/256 Director.

The 4/256 Director allows you to use chassis configuration options 1 and 5. Configuration option 1 is compatible with FC2-16 and FC4-16 blades; configuration option 5 is compatible with FC8-16, FC4-16IP, FC4-16, FC4-32, FR4-18i, and FC4-48 blades.

The DC Director does not have separate configuration options, so the chassisConfig command is not supported on this platform. By default the DC Director supports 384 ports in a single Fibre Channel domain.

Table 55 lists the supported configuration options for the 4/256 Director.

Table 55 Supported configuration options

<table>
<thead>
<tr>
<th>Option</th>
<th>Number of domains</th>
<th>Maximum number of ports per switch</th>
<th>Supported port blades</th>
<th>Supported CP blades</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>128</td>
<td>FC2-16, FC4-16</td>
<td>CP2 or CP4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>384</td>
<td>FC4-16, FC8-16, FC4-16IP, FC4-32, FC4-48, FR4-18i</td>
<td>CP4</td>
<td>Option 5 is the default configuration option for 4/256 Director.</td>
</tr>
</tbody>
</table>

¹. L_Ports are not supported on the FC4-48 blade.
Table 56 lists chassis configuration options and resulting slot configurations.

### Table 56  Chassis configuration options

<table>
<thead>
<tr>
<th>Option</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>One 128-port switch (Blade IDs 4, 17 on slots 1–4, 7–10. Blade ID 5 and 16 on slots 5, 6)</td>
</tr>
<tr>
<td>5</td>
<td>One 384-port switch (Blade IDs 4, 17, 18, 31, and 36 on slots 1–4, 7–10. Blade ID 16 on slots 5, 6)</td>
</tr>
</tbody>
</table>

See Table 53 for details about the different blades, including their corresponding IDs.

**Obtaining slot information**

To display the status of all slots in the chassis:

1. Connect to the switch and log in as user or admin.
2. Enter the `slotShow` command to display the current status of each slot in the system. The format of the display includes a header and four fields for each slot. The fields and their possible values are:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Displays the physical slot number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blade</td>
<td>Displays the blade type:</td>
</tr>
<tr>
<td>Type</td>
<td>SW BLADE: The blade is a port blade.</td>
</tr>
<tr>
<td></td>
<td>CP BLADE: The blade is a control processor.</td>
</tr>
<tr>
<td></td>
<td>CORE BLADE: The blade is a core blade (DC Director only).</td>
</tr>
<tr>
<td></td>
<td>AP BLADE: The blade is the FR4-18i blade.</td>
</tr>
<tr>
<td></td>
<td>UNKNOWN: The blade is not present or its type is not recognized.</td>
</tr>
<tr>
<td>ID</td>
<td>Displays the hardware ID of the blade type.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the blade:</td>
</tr>
<tr>
<td></td>
<td>VACANT: The slot is empty.</td>
</tr>
<tr>
<td></td>
<td>INSERTED, NOT POWERED ON: The blade is present in the slot but is turned off.</td>
</tr>
<tr>
<td></td>
<td>POWERING UP: The blade is present and powering on.</td>
</tr>
<tr>
<td></td>
<td>LOADING: The blade is present, powered on, and loading initial configuration.</td>
</tr>
<tr>
<td></td>
<td>DIAG RUNNING POST1: The blade is present, powered on, and running the post-initialization power-on self test (POST).</td>
</tr>
<tr>
<td></td>
<td>DIAG RUNNING POST2: The blade is present, powered on, and running the POST.</td>
</tr>
<tr>
<td></td>
<td>INITIALIZING: The blade is present, powered on, and initializing hardware components.</td>
</tr>
<tr>
<td></td>
<td>ENABLED: The blade is on and enabled.</td>
</tr>
<tr>
<td></td>
<td>ENABLED (User Ports Disabled): The blade is on, but external ports have been disabled with the <code>bladeDisable</code> command.</td>
</tr>
<tr>
<td></td>
<td>DISABLED: The blade is powered on but disabled.</td>
</tr>
<tr>
<td></td>
<td>FAULTY: The blade is faulty because an error was detected. The reason code numbers displayed are used by Support personnel to assist with problem diagnosis. Review the system error logs for more information.</td>
</tr>
<tr>
<td></td>
<td>UNKNOWN: The blade is inserted but its state cannot be determined.</td>
</tr>
</tbody>
</table>
9 Routing traffic

This chapter provides information on routing policies.

About data routing and routing policies

Data moves through a fabric from switch to switch and from storage to server along one or more paths that make up a route. Routing policies determine the correct path for each frame of data.

Whatever routing policy a switch is using applies to the VE_Ports as well. See “Using the FC-FC routing service” on page 215 for details about VE_Ports.

TIP: For most configurations, the default routing policy is optimal, and provides the best performance. You should only change the policy if there is a performance issue that is of concern, or a particular fabric configuration requires it.

The following routing policies are available to tune routing performance:

- Exchange-based routing
  The choice of routing path is based on the Source ID (SID), Destination ID (DID), and Fibre Channel originator exchange ID (OXID), optimizing path utilization for the best performance. Thus, every exchange can take a different path through the fabric. Exchange-based routing requires the use of the Dynamic Load Sharing (DLS) feature; when these policies are in effect, you cannot disable the DLS feature.

- Port-based routing
  The choice of routing path is based only on the incoming port and the destination domain. To optimize port-based routing, DLS can be enabled to balance the load across the available output ports within a domain.

  Using port-based routing, you can assign a “static route,” in which the path chosen for traffic never changes. In contrast, exchange-based routing policies always employ “dynamic path selection.”

Port-based routing is supported by all HP models.

Specifying the routing policy

The following routing policies are supported:

- Port-based path selection
  This is the default on 4/256 SAN Director (using configuration option 1). When using configuration option 1, these directors support the port-based policy only; you cannot change the routing policy for these directors.


- Exchange-based path selection
  This is the default on HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP cClass BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router and 4/256 SAN Director (using configuration option 5), and DC SAN Backbone Director (short name, DC Director).

  See “Configuring Directors” on page 25 for more details about 4/256 SAN Director configuration options.

You can use the aptPolicy command to display and specify a different routing policy. The aptPolicy command detects the switch’s configuration options and provides the appropriate policies for users to select from. For example, if you attempt to set the policy for the 4/256 SAN Director using configuration
option 1, an error message is returned because you cannot change the routing policy. See the Fabric OS Command Reference for more details on the aptPolicy command.

You must disable the switch before changing the routing policy, and re-enable it afterward.

Assigning a static route

A static route can be assigned only when the active routing policy is port-based and running on an HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch., Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP c-Class BladeSystem, SAN Switch 4/32, SAN Switch 4/32B, or 4/256 SAN Director (using configuration option 1). When exchange-based routing is active, you cannot assign static routes. Even if the active routing policy is port-based, you cannot assign static routing to the 4/64 SAN Switch, 400 Multi-protocol Router, 4/256 SAN Director (using configuration option 5), or DC Director.

To assign a static route, use the uRouteConfig command. To remove a static route, use the uRouteRemove command.

**NOTE:** For the 4/256 SAN Director (using configuration option 1):

When you enter the uRouteConfig command, two similar warning messages may display if a platform conflict occurs. The first message displays when the static routing feature detects the conflict. The second message displays when the Dynamic Load Sharing feature detects the condition as it tries to rebalance the route.

A platform conflict occurs if a static route was configured with a destination port that is currently down. The static route is ignored in this case, in favor of a normal dynamic route. When the configured destination port comes back up, the system attempts to re-establish the static route, potentially causing a conflict.

Specifying frame order delivery

The order of delivery of frames is maintained within a switch and determined by the routing policy in effect. The frame delivery behaviors for each routing policy are:

- **Port-based routing**
  All frames received on an incoming port destined for a destination domain are guaranteed to exit the switch in the same order in which they were received.

- **Exchange-based routing**
  All frames received on an incoming port for a given exchange are guaranteed to exit the switch in the same order in which they were received. Because different paths are chosen for different exchanges, this policy does not maintain the order of frames across exchanges.

If even one switch in the fabric delivers out-of-order exchanges, then exchanges are delivered to the target out-of-order, regardless of the policy configured on other switches in the fabric.

**NOTE:** Some devices do not tolerate out-of-order exchanges; in such cases, use the port-based routing policy.

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for example, if a link goes down), traffic is rerouted around the failure, and some frames could be delivered out of order. Most destination devices tolerate out-of-order delivery, but some do not.

By default, out-of-order frame-based delivery is allowed to minimize the number of frames dropped. Enabling in-order delivery (IOD) guarantees that frames are either delivered in order or dropped. You should only force in-order frame delivery across topology changes if the fabric contains destination devices that cannot tolerate occasional out-of-order frame delivery.
To force in-order frame delivery across topology changes:

1. Connect to the switch and log in as admin.
2. Enter the `iodSet` command at the command line.

**NOTE:** This command can cause a delay in the establishment of a new path when a topology change occurs; use it with care.

3. To confirm the in-order delivery has been set, issue the `iodShow` command.

To restore out-of-order frame delivery across topology changes:

1. Connect to the switch and log in as admin.
2. Enter the `iodSet` command at the command line.

### Using dynamic load sharing

The exchange-based routing policy depends on the Fabric OS Dynamic Load Sharing feature (DLS) for dynamic routing path selection. When using the exchange-based routing policy, DLS is by default enabled and cannot be disabled. In other words, you cannot enable or disable DLS when the exchange-based routing policy is in effect.

When the port-based policy is in force, you can enable DLS to optimize routing. When DLS is enabled, it shares traffic among multiple equivalent paths between switches. DLS recomputes load sharing when a switch boots up or each time an E_Port goes offline and online, or an EX_Port goes offline.

To check and set DLS:

1. Connect to the switch and log in as admin.
2. Enter the `dlsShow` command to view the current DLS setting.
   
   One of the following messages appears:
   
   - “DLS is set” indicates that dynamic load sharing is turned on.
   - “DLS is not set” indicates that dynamic load sharing is turned off.
   - “DLS cannot be changed with current routing policy” indicates that you are using the exchange-based routing policy and you cannot enable or disable DLS. If you get this message, you cannot perform step 3, so you are done with this procedure.

3. Enter the `dlsSet` command to enable DLS or enter the `dlsReset` command to disable it.

```
switch:admin> dlsshow
DLS is not set
switch:admin> dlsset
switch:admin> dlsshow
DLS is set
switch:admin> dlsreset
switch:admin> dlsshow
DLS is not set
```
Viewing routing path information

The `topologyShow` and `uRouteShow` commands provide information about the routing path.

1. Connect to the switch and log in as admin.
2. Enter the `topologyShow` command to display the fabric topology, as it appears to the local switch:

```
switch:admin> topologyshow
```

4 domains in the fabric; Local Domain ID: 2

Domain:         1
Metric:         10500
Name:           fcr_xd_1_1
Path Count:     1
Hops:                   2
Out Port:               39
In Ports:               35 56
Total Bandwidth:        4.000 Gbps
Bandwidth Demand:       300 %
Flags:                  D

The following information displays:

- **Local Domain ID**: The domain number of the local switch.
- **Domain**: The domain number of the destination switch.
- **Metric**: The cost of reaching the destination domain.
- **Name**: The name of the destination switch.
- **Path Count**: The number of currently active paths to the destination domain.
- **Hops**: The maximum number of switch-to-switch links (ISLs) transversed to reach the destination domain.
- **Out Port**: The port to which the incoming frame will be forwarded in order to reach the destination domain.
- **In Ports**: The input ports that use the corresponding Out Port to reach the destination domain.
- **Total Bandwidth**: The maximum bandwidth of the out port.
- **Bandwidth Demand**: The maximum bandwidth demand of the in ports.
- **Flags**: An indication whether the route is dynamic (D) or static (S). This value is always “D”, indicating a dynamic path.
3. Use the `urouteShow` command to display unicast routing information for the following:

   HP StorageWorks 4/8 SAN Switch and 4/16 SAN Switch, SAN Switch 4/32, Brocade
   4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP
   c-Class BladeSystem, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol
   Router

   Use the following syntax:

   `urouteShow [portnumber] [, domainnumber]`

   **4/256 SAN Director and DC Director**: Use the following syntax:

   `urouteShow [slot/] [portnumber] [, domainnumber]`

The following information displays:

- **Local Domain ID**: The domain number of the local switch.
- **In Port**: The port from which a frame is received.
- **Domain**: The destination domain of the incoming frame.
- **Out Port**: The port to which the incoming frame will be forwarded in order to
  reach the destination domain.
- **Metric**: The cost of reaching the destination domain.
- **Hops**: The maximum number of switch-to-switch links (ISLs) transversed to
  reach the destination domain.
- **Flags**: An indication whether the route is dynamic (D) or static (S). A static
  route is assigned using the command `uRouteConfig`.
- **Next (Dom, Port)**: The domain number and port number of the next hop.

The following example displays the routing information of all the active ports:

```
switch:admin> urouteShow

Local Domain ID: 1

<table>
<thead>
<tr>
<th>In Port</th>
<th>Domain</th>
<th>Out Port</th>
<th>Metric</th>
<th>Hops</th>
<th>Flags</th>
<th>Next (Dom, Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>4</td>
<td>9</td>
<td>500</td>
<td>1</td>
<td>D</td>
<td>4,24</td>
</tr>
</tbody>
</table>

switch:admin>
```

The next example displays the routing information for port 11 on slot 1:

```
switch:admin> urouteShow 1/11

Local Domain ID: 3

<table>
<thead>
<tr>
<th>In Port</th>
<th>Domain</th>
<th>Out Port</th>
<th>Metric</th>
<th>Hops</th>
<th>Flags</th>
<th>Next (Dom, Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>2</td>
<td>0</td>
<td>1500</td>
<td>2</td>
<td>D</td>
<td>4,0</td>
</tr>
<tr>
<td>4</td>
<td>16</td>
<td>500</td>
<td>1</td>
<td>D</td>
<td></td>
<td>4,0</td>
</tr>
</tbody>
</table>

switch:admin>
```

This example displays the routing information of port 11 to domain 4 only:

```
switch:admin> urouteShow 1/11, 4

Local Domain ID: 3

<table>
<thead>
<tr>
<th>In Port</th>
<th>Domain</th>
<th>Out Port</th>
<th>Metric</th>
<th>Hops</th>
<th>Flags</th>
<th>Next (Dom, Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>4</td>
<td>16</td>
<td>500</td>
<td>1</td>
<td>D</td>
<td>4,0</td>
</tr>
</tbody>
</table>
```

Fabric OS 6.x administrator guide 211
Viewing routing information along a path

You can display detailed routing information from a source port (or area) on the local switch to a destination port (or area) on another switch. This routing information describes the full path that a data stream travels between these ports, including all intermediate switches.

1. Connect to the switch and log in as admin.
2. Enter the `pathInfo` command. In interactive mode, you can specify the following parameters for display:

   - **Max hops**: The maximum number of hops that the pathInfo frame is allowed to traverse.
   - **Domain**: The destination Domain ID.
   - **Source Port**: The port number (or area number for 4/256 SAN Director) on which the switch receives frames.
   - **Destination Port**: The output port the frames use to reach the next hop on this path. For the last hop, the destination port.
   - **Basic stats**: Basic statistics on every link.
   - **Extended stats**: Detailed statistics on every link.
   - **Trace reverse path**: Whether the same path should be followed from the destination switch back to the source switches.
   - **Source route**: Whether the frame should follow a specified path to reach the destination.
   - **Timeout**: The maximum time to wait for a response from `pathInfo`, in seconds.

Paths always originate on the local switch. The path destination can be specified by domain or port. By default, the path will be the path taken by traffic from the source to destination port, but you can also specify all or portions of a path.

See the Fabric OS Command Reference for details on the `pathInfo` command.

Following is an example of `pathInfo` in interactive mode.

```
switch:admin> pathinfo

Max hops: (1..127) [25]
Domain: (1..239) [-1] 1
Source port: (0..255) [-1] -
Destination port: (0..255) [-1] -
Basic stats (yes, y, no, n): [no]
Extended stats (yes, y, no, n): [no]
Trace reverse path (yes, y, no, n): [no]
Source route (yes, y, no, n): [no]
Timeout: (1..30) [10]

Target port is Embedded

<table>
<thead>
<tr>
<th>Hop</th>
<th>In Port</th>
<th>Domain ID (Name)</th>
<th>Out Port</th>
<th>BW</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>E</td>
<td>10 (web226)</td>
<td>15</td>
<td>2G</td>
<td>500</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td>1 (web229)</td>
<td>E</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
```

212 Routing traffic
The information that `pathInfo` provides is:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hops</td>
<td>The number of switch-to-switch links (ISLs) traversed. The local switch is hop 0.</td>
</tr>
<tr>
<td>In Port</td>
<td>The port that the frames come in from on this path. For hop 0, the source port.</td>
</tr>
<tr>
<td>Domain ID</td>
<td>The Domain ID of the switch.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the switch.</td>
</tr>
<tr>
<td>Out Port</td>
<td>The output port that the frames use to reach the next hop on this path. For the last hop, the destination port.</td>
</tr>
<tr>
<td>BW</td>
<td>The bandwidth of the output ISL, in Gbps. It does not apply to the embedded port.</td>
</tr>
<tr>
<td>Cost</td>
<td>The cost of the ISL used by FSPF routing protocol. It applies only to an E_Port.</td>
</tr>
</tbody>
</table>
10 Using the FC-FC routing service

Supported platforms

FC-FC Routing is supported on the following platforms:

- 400 MP Router
- 4/256 SAN Director or DC SAN Backbone Director (short name, DC Director) when it is configured with an FR4-18i blade and uses chassis configuration option 5

**NOTE:** The DC Director only supports chassis configuration option 5.

Supported configurations

In an edge fabric that contains a mix of administrative domain (AD)-capable switches and switches that are not aware of AD, the FC router must be connected directly to the AD-capable switch. For more information, see “Use of administrative domains with LSAN zones and FCR” on page 235.

You can use SANtelligence to configure M-Series switches connecting to a B-Series router. For more information, refer to “Implementing an interoperable fabric” on page 481.

The supported configurations are:

- FC router connected to an HP nonsecured fabric.
- FC router connected to an HP secured fabric.
- FC router connected to a McDATA fabric configured for Open Mode 1.
- FC router connected to a McDATA fabric configured for McDATA fabric mode.
- FC router connected to HP secured and nonsecured fabrics with EX_Port trunking enabled.
- FC router interoperating with older FC routers (XPath OS 7.4.x and Fabric OS 5.1, 5.2, and 5.3).

Fibre Channel routing concepts

Fibre Channel routing introduces the following concepts:

- Backbone Fabric
  A backbone (BB) fabric is an intermediate network that connects one or more edge fabrics. In a SAN, the backbone fabric consists of at least one FC router and possibly a number of Fabric OS-based Fibre Channel switches (see Figure 10).
  
  While the 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade facilitate communication between devices in edge fabrics with those in a backbone fabric, this is not true of the Multi-protocol Router.

- Edge Fabric
  An edge fabric is a Fibre Channel fabric with targets and initiators connected through the supported platforms by using an EX_Port or VEX_Port.

- EX_Port, VEX_Port
  Special types of ports, called an EX_Port and a VEX_Port, function similarly to an E_Port and VE_Port respectively, but terminate at the switch and do not propagate fabric services or routing topology information from one edge fabric to another. The link between an E_Port and EX_Port, or VE_Port and VEX_Port, is called an interfabric link (IFL). You can configure multiple IFLs from a 400 MP Router, an FR4-18i operating in a 4/256 SAN Director or DC Director using chassis configuration option 5, from additional HP routers, or from all three. These are referred to as “an FC router” throughout this chapter and unless specified, any FC router can be used.

  FC-FC Routing Services support EX_Ports and VEX_Ports connected to the same edge fabrics (see Figure 8). See “Configuring and monitoring FCIP extension services” on page 333 for details about VE_Ports.
Figure 8 shows a metaSAN consisting of three edge fabrics connected through a 4/256 SAN Director or DC Director containing an FR4-18i with interfabric links.

- **Fabric ID (FID) U R HERE**
  Every EX_Port and VEX_Port uses the fabric ID (FID) to identify the fabric at the opposite end of the IFL. Configure all of the EX_Ports and VEX_Ports attached to the same edge fabric with the same FID. The FID for every edge fabric must be unique from each backbone fabric’s perspective. Configure the FID for all of the EX_Ports and VEX_Ports from a backbone fabric to uniquely reference each of the attached edge fabrics.
  When two different backbones are connected to the same edge fabric, the backbone fabric IDs must be different but the edge fabric ID must be the same. Configuring the same backbone fabric ID for two backbones that are connected to the same edge is invalid. In this configuration, a RASLog message displays a warning about fabric ID overlap.
  Backbone fabrics which share connections to the same edge fabrics must have unique backbone fabric IDs.

- **Fibre channel router**
  A switch running the FC-FC routing service.

- **Logical storage area networks (LSANs)**
  An LSAN is defined by zones in two or more edge or backbone fabrics that contain the same devices. You can create LSANs that can span fabrics. These LSANs enable Fibre Channel zones to cross physical SAN boundaries without merging the fabrics while maintaining the access controls of zones (see Figure 9).
  An LSAN device can be a “physical device,” meaning that it physically exists in the fabric, or it can be a proxy device. A proxy device represents a real device in a remote fabric. It has a name server entry and is assigned a valid port ID. When a proxy device is created in a fabric, the real device is considered to be imported into this fabric. The presence of a proxy device is required for interfabric device communication.
Figure 9 shows a metaSAN with a backbone consisting of one 400 MP Router connecting hosts in Edge Fabrics 1 and 3 with storage in Edge Fabric 2 and the backbone through the use of LSANs. There are devices shared between the backbone and Edge Fabric 1, between Edge Fabric 1 and Edge Fabric 2, and between Edge Fabric 2 and Edge Fabric 3.

- **MetaSAN**
  A metaSAN is the collection of all SANs interconnected with Fibre Channel routers. A simple metaSAN can be constructed using a 400 MP Router, the 4/256 SAN Director or DC Director with an FR4-18i to connect two or more separate fabrics. Additional FC routers can be used to increase the available bandwidth between fabrics and to provide redundancy.

- **Proxy device**
  A proxy device is a virtual device imported into a fabric by a Fibre Channel router, and represents a real device on another fabric. When a proxy device is created in a fabric, the real Fibre Channel device is considered to be imported into this fabric. The presence of a proxy device is required for interfabric device communication.

- **Proxy PID**
  A proxy PID is the port ID (PID) of the proxy device. The proxy device appears to the fabric as a real Fibre Channel device, has a name server entry, and is assigned a valid port ID. The port ID is only relevant on the fabric in which the proxy device has been created.

- **Phantom domains**
  A phantom domain is a domain emulated by the Fibre Channel router. The FC router can emulate two types of phantom domains. The first set of phantom domains are known as front phantom domains. There is one front phantom domain from the FCR to an edge fabric.
  
  The second level of phantom domains is known as a translate phantom domain. The EX_Ports also present translate phantom domains in edge fabrics as being topologically behind the front domains; if the translate phantom domain is in a backbone fabric, then it is topologically present behind the Fibre Channel router because there is no front domain in a backbone fabric. The translate phantom domain is a router virtual domain that represents an entire fabric. Device connectivity can be achieved from one fabric to another—over the backbone or edge fabric through this virtual domain—without merging the two fabrics. Translate phantom domains are sometimes referred to as translate domains or xlate domains.
If an FR4-18i blade is attached to an edge fabric using an EX_Port, it will create translate phantom domains in the fabric corresponding to the imported edge fabrics with active LSANs defined. If you import devices into the backbone fabric, then a translate phantom domain is created in the backbone device in addition to the one in the edge fabric.

If you lose connectivity to the edge fabric due to link failures or disabling the IFL, by issuing the `portDisable` command from the switch in the attached fabric, translate phantom domains remain visible. This prevents unnecessary fabric disruptions caused by translate phantom domains repeatedly going offline and online due to corresponding IFL failures. To remove the translate phantom domain from the backbone, disable all EX_Ports or VEX_Ports through which the translate phantom domain was created.

Figure 10 shows another metaSAN consisting of a host in Edge SAN 1 connected to storage in Edge SAN 2 through a backbone fabric connecting two 4/256 SAN Director, each containing an FR4-18i.

**Proxy devices**

A 400 MP Router, 4/256 SAN Director or DC Director with an FR4-18i achieves interfabric device connectivity by creating proxy devices (hosts and targets) in attached fabrics that represent real devices in other fabrics. For example, a host in Fabric 1 can communicate with a target in Fabric 2 as follows:

- A proxy target in Fabric 1 represents the real target in Fabric 2.
- Likewise, a proxy host in Fabric 2 represents the real host in Fabric 1.

The host discovers and sends Fibre Channel frames to the proxy target. The 400 MP Router, 4/256 SAN Director or DC Director with an FR4-18i receives these frames, translates them appropriately, then delivers them to the destination fabric for delivery to the target.

The target responds by sending frames to the proxy host. Hosts and targets are exported from the edge SAN to which they are attached and, correspondingly, imported into the edge SAN reached through Fibre Channel routing. Figure 11 illustrates this concept.
Routing types

- **Edge-to-Edge**
  Occurs when devices in one edge fabric communicate with devices in another edge fabric through one or more Fibre Channel routers.

- **Backbone-to-Edge**
  Occurs when Fibre Channel routers connect to a common fabric—known as a backbone fabric—through E_Ports. A backbone fabric can be used as a transport fabric that interconnects edge fabrics. Fibre Channel routers also enable hosts and targets in edge fabrics to communicate with devices in the backbone fabric, known as **backbone-to-edge routing**. From the edge fabric’s perspective, the backbone fabric is just like any other edge fabric. For the edge fabric and backbone fabric devices to communicate, the shared devices need to be presented to each other’s native fabric. To do so, at least one translate phantom domain is created in the backbone fabric. This translate phantom domain represents the entire edge fabric. The shared physical devices in the edge have corresponding proxy devices on the translate phantom domain.

  Each edge fabric has one and only one xlate domain to the backbone fabric. The backbone fabric device communicates with the proxy devices whenever it needs to contact the shared physical devices in the edge. The FC-FC Routing Service receives the frames from the backbone switches destined to the proxy devices, and redirects the frames to the actual physical devices. As with an edge fabric, the translate phantom domain can never be the principal switch of the backbone fabric. Front domains are not created; rather, only translate phantom domains are created in the backbone fabric.

  Devices are exported from the backbone fabric to one or more edge fabrics using LSANs. See “Configuring LSANs and zoning” on page 235 for more information.

  **NOTE:** Secure Fabric OS, Management Server Platform services, and interopmode are not supported in the backbone fabric.

**Fibre Channel NAT and phantom domains**

Within an edge fabric or across a backbone fabric, the standard Fibre Channel fabric shortest path first (FSPF) protocol determines how frames are routed from the source Fibre Channel device to the destination FC device. The source or destination device can be a proxy device. When frames traverse the fabric through a 400 MP Router, 4/256 SAN Director or DC Director with an FR4-18i in the backbone (BB), the frames are routed to another EX_Port or VEX_Port.
Fibre Channel fabrics require that all ports be identified by a unique PID. In a single fabric, FC protocol guarantees that Domain IDs are unique, and so a PID formed by a Domain ID and area ID is unique within a fabric. However, the Domain IDs and PIDs in one fabric may be duplicated within another fabric, just as IP addresses are unique to one private network are likely to be duplicated within another private network.

In an IP network, a network router can maintain network address translation (NAT) tables to replace private network addresses with public addresses when a packet is routed out of the private network, and to replace public addresses with private addresses when a packet is routed from the public network to the private network. The Fibre Channel routing equivalent to this IP-NAT is the Fibre Channel network address translation (FC-NAT). Using FC-NAT, the proxy devices in a fabric can have different PIDs than the real devices that they represent, allowing the proxy devices to have appropriate PIDs for the address space of their corresponding fabric.

All EX_Ports connected to the same edge fabric from one physical FC router present a single front phantom domain and one additional translate (xlate) phantom domain for each edge fabric accessed through it. All EX_Ports and VEX_Ports connected to an edge fabric use the same xlate Domain ID number for an imported edge fabric; this value persists across switch reboots and fabric reconfigurations. Xlate domains are presented as being connected topologically behind one or more front domains; each FC-Router presents one front domain to the edge fabric. This allows redundant paths in remote fabrics to present themselves as redundant paths to proxy devices in an edge fabric.

Phantom domains are like logical switches that appear to be connected to an edge fabric through the front domains that are presented by EX_Ports and VEX_Ports. The combination of front domains and xlate domains allows routing around path failures, including path failures through the routers. The multiple paths to a xlate domain provide additional bandwidth and redundancy.

There are some differences in how the xlate domain is presented in the BB. The BB xlate domains are topologically connected to FC routers and participate in FC-Protocol in the BB. Front domains are not needed in the BB. As in the case of a xlate domain in edge fabric, BB xlate domains provide additional bandwidth and redundancy by being able to present themselves as being connected to single or multiple FC routers with each FC router capable of connecting multiple IFLs to edge fabrics.

**Setting up the FC-FC routing service**

To set up the FC-FC Routing Service, perform the following tasks:

1. “Performing verification checks” on page 221 next
2. “Assigning backbone fabric IDs” on page 222
3. “Configuring FCIP tunnels (optional)” on page 223
4. “Configuring FC-FC routing to work with Secure Fabric OS (optional)” on page 223
5. “Configuring an interfabric link” on page 225
6. “Configuring the FC Router port cost (optional)” on page 230
7. “Configuring EX_Port frame trunking (optional)” on page 233
8. “Configuring LSANs and zoning” on page 235

See “Configuring Directors” on page 25 for more details about configuration options for Directors.
Performing verification checks

Before configuring a fabric to connect to another fabric, you must perform the following verification checks on the switch or director.

To perform verification checks:

1. Log in to the switch or director as admin and enter the `version` command. Verify that Fabric OS 6.0 is installed on the 400 MP Router, 4/256 SAN Director or DC Director with the FR4-18i blade as shown in the following example.

```
switch:admin_06> version
Kernel: 2.4.19
Fabric OS: v6.0
Made on: Mon Sep 24 01:15:34 2007
Flash: Tue Sep 25 20:53:48 2007
BootProm: 4.5.3
```

2. If configuring the 4/256 SAN Director or DC Director with an FR4-18i blade, enter the `slotShow` command to verify that the FR4-18i blade is present. The following example shows slot 2 with AP blade 24 enabled.

```
switch:admin_06> slotShow
Slot  Blade Type   ID    Status
---------------------------------
 1     SW BLADE   17     ENABLED
 2     AP BLADE   24     ENABLED
 3     UNKNOWN           VACANT
 4     UNKNOWN           VACANT
 5     CP BLADE   16     ENABLED
 6     CP BLADE   16     ENABLED
 7     SW BLADE   17     ENABLED
 8     UNKNOWN           VACANT
 9     SW BLADE   18     ENABLED
10    UNKNOWN           VACANT
```

See “Configuring Directors” on page 25 for a list of blades and their corresponding IDs.

3. If configuring the 4/256 SAN Director with an FR4-18i blade, then enter the `chassisConfig` command to verify that the director is using configuration option 5.

```
NOTE: The DC Director only supports chassis configuration option 5.
```

```
switch:admin> chassisconfig
Current Option: 5

All Supported Options
----------------------------------------------
Option 1: One 128-port switch
   Blade ID's 4, 17 in slots 1-4, 7-10
   Blade ID's 5, 16 in slots 5-6
Option 5: One 256-port switch
   Blade ID's 17, 18, 24 in slots 1-4, 7-10
   Blade ID 16 in slots 5-6

Please use slotShow to see Blade IDs currently in the system.
```
4. Enter the `interopMode` command and verify that Brocade switch interoperability with switches from other manufacturers is disabled.

```
switch:admin> interopmode
InteropMode: Off
```

Usage: InteropMode 0|1
0: to turn it off
1: to turn it on

5. Enter the `msPlatShow` command to verify that Management Server Platform database is disabled in the backbone fabric.

```
switch:admin_06> msplatshow
*MS Platform Management Service is NOT enabled.
```

If any of the items listed in the prior steps are enabled, you can see the Fabric OS Command Reference for information on how to disable the option. For information about security, see “Configuring standard security features” on page 69 and “Configuring advanced security features” on page 99.

When it is in strict mode, ACL cannot support Fibre Channel routing in the fabric. Before connecting an edge fabric to an FC router and before setting up the FC router in the BB, verify that the Fabric Wide Consistency Policy is not in 'strict' mode by issuing the `fddCfg --showall` command.

```
switch:admin> fddcfg --showall
Local Switch Configuration for all Databases:-
DATABASE - Accept/Reject
---------------------------------------
SCC - accept
DCC - accept
PWD - accept
Fabric-Wide Consistency Policy :- "SCC:S;DCC"
```

If the Fabric Wide Consistency Policy has the ‘S’ letter in it in the edge fabric or the BB fabric, do not connect the edge fabric or the BB to the FC router. See the Fabric OS Command Reference for details.

### Assigning backbone fabric IDs

If your configuration has only one backbone fabric, then this task is not required because the backbone fabric ID in this situation defaults to a value of 1.

All switches in a backbone fabric must have the same backbone fabric ID. You can configure the backbone fabric ID using the `fcrConfigure` command. The backbone fabric ID is required to be unique from the perspective of every attached edge fabric. Fabric ID changes made on a switch are not propagated to other switches in the backbone fabric. Rather, the backbone fabric administrator is responsible for making sure that all switches in the backbone have the same fabric ID. Because fabric IDs are used heavily by the routing protocol between the Fibre Channel routers, using the wrong fabric ID can affect both edge-to-edge and backbone-to-edge routing.

In addition to ensuring that the backbone fabric IDs are the same within the same backbone, you need to make sure that when two different backbones are connected to the same edge fabric, the backbone fabric IDs are different, but the edge fabric ID should be the same. Configuration of two backbones with the same backbone fabric ID that are connected to the same edge is invalid. In this configuration, a RASLog message displays a warning about fabric ID overlap. However, when two backbone fabrics are not connected to the same edge, they can have the same backbone fabric ID.

**IMPORTANT:** In a multi-switch backbone fabric, modification of FID within the backbone fabric will cause disruption to local traffic.
To assign backbone fabric IDs:

1. Log in to the switch or director.
2. Enter the `fosConfig --disable fcr` command to disable the FC-FC Routing Service. See the Fabric OS Command Reference or the CLI man pages for more information about the `fosConfig` command.

**NOTE:** The default state for the FCR is disabled. The `fcrEnable` and `fcrDisable` commands continue to operate as before in Fabric OS versions 5.2.0 and earlier.

The `fosConfig` command is the only method for enabling and disabling the FC-FC Routing Service in Fabric OS 6.0 and is also supported in 5.3.0.

3. Enter the `fcrConfigure` command. At the prompt, enter the fabric ID, or press `Enter` to specify the default fabric ID (1).
4. Verify the backbone fabric ID is different from that set for edge fabrics. Multiple FC routers attached to the same backbone fabric must have the same backbone fabric ID.
5. Enter the `fosConfig --enable` command.

```bash
switch:admin> fosconfig --disable fcr
FC router service is disabled

switch:admin> fcrconfigure
FC router parameter set. <cr> to skip a parameter
Backbone fabric ID: (1-128)[1]

switch:admin> fosconfig --enable fcr
FC router service is enabled
```

**Configuring FCIP tunnels (optional)**

The optional Fibre Channel over IP (FCIP) Tunneling Service enables you to use “tunnels” to connect instances of Fibre Channel SANs over IP-based networks to transport all Fibre Channel ISL and IFL traffic. FCIP is a prerequisite for configuring VEX_Ports; if you are only using FC_Ports, then there is no need to perform this step.

If using FCIP in your FC-FC Routing configuration, you must first configure FCIP tunnels. Once a tunnel is created, it defaults to a disabled state. Then configure the VE_Port or VEX_Port. After the appropriate ports are configured, enable the tunnel.

**NOTE:** This section is applicable only to Fabric OS fabrics and does not apply to M-EOS fabrics.

See "Configuring and monitoring FCIP extension services" on page 333 for instructions on how to configure FCIP tunnels.

**Configuring FC-FC routing to work with Secure Fabric OS (optional)**

If you do not have Secure Fabric OS enabled in the edge fabric, then you are not required to complete the tasks in this section.

**NOTE:** Secure Fabric OS is not supported in backbone fabrics. You can connect a Fibre Channel router to an edge fabric that has security enabled, although this is not a prerequisite for FCR to work.

The 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade support Fibre Channel routing between secure fabric employing Secure Fabric OS with DH-CHAP (Diffie-Hellman with Challenge-Handshake Authentication Protocol) authentication. It also supports secure fabric to nonsecure
fabrics. Secure Fabric OS is an optional licensed product that provides customizable security restrictions through local and remote management channels on an HP fabric.

Although Secure Fabric OS is not supported in Fabric OS 6.0, you can still connect a 6.0 switch to an edge switch that participates in a Secure Fabric OS.

The FC-FC Routing Service uses only the DH-CHAP shared secrets to provide switch-to-switch authentication when connecting to a Secure Fabric OS fabric. You can set up DH-CHAP on the edge fabric, but it is not a prerequisite for FCR to work.

To determine whether an EX_Port or VEX_Port is connected to a Secure Fabric OS fabric, enter the `portShow`, `portCfgEXPort`, or `portCfgVEXPort` command, as described in the Fabric OS Command Reference. Note that you should issue these commands only after the IFLs have been configured for the EX_ and VEX_ Ports and the FCIP tunnels are up and running. For more details, see “Configuring an interfabric link” on page 225 and “Configuring FCIP tunnels (optional)” on page 223.

Configuring DH-CHAP secret

While Secure Fabric OS supports the SLAP, FCAP and DH-CHAP authentication protocols to communicate with each switch, Fabric OS 6.0 supports only DH-CHAP.

The 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade do not initiate DH-CHAP authentication requests; rather, they respond to DH-CHAP requests only from the edge switch to which they are connected—in this case, the Secure Fabric OS switch.

As soon as you connect the 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade to a Secure Fabric OS switch, DH-CHAP authentication is initiated.

The DH-CHAP secrets are configured both on the Secure Fabric OS switch and the 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade. Each entry specifies the WWN of the peer to which it is connected. For example, on the 4/256 SAN Director or DC Director with an FR4-18i blade, specify the WWN of the Secure Fabric OS switch and the secrets. On the Secure Fabric OS switch, specify the WWN of the front domain (EX_Port or VEX_Port) and the secrets. To view the front domain WWN, issue the `portCfgEXPort` command on the Fibre Channel router side.

The WWN of the front domain (EX_Port or VEX_Port) that is connected to the Secure Fabric OS switch should be present in the Switch Connection Controls (SCC) list. See the Secure Fabric OS Administrator’s Guide for details about the SCC and other Secure Fabric OS features.

To configure a DH-CHAP secret word:

1. Log in to the 400 MP Router, 4/256 SAN Director or DC Director with an FR4-18i blade with administrative privileges.
2. At the Telnet prompt, enter the `secAuthSecret` command. The secret must be between 8 and 40 characters long.
   Setting up secret keys does not initiate DH-CHAP authentication. DH-CHAP authentication is performed whenever a port or a switch is enabled.
3. Follow the instructions provided on screen.
   a. Type the port or switch WWN.

**NOTE:** Use only the WWN as the input. The Domain ID or switch name is not acceptable.

   b. Type and confirm the peer secret.
   c. Type and confirm the local secret.
4. After you have added all of the DH-CHAP secret information, press **Enter** to indicate that you have completed the secret key setup.
5. When prompted, type y. The DH-CHAP secret is now stored in the secret word database and is ready for use.

```
switch:admin> secauthsecret --set
```

This command is used to set up secret keys for the DH-CHAP authentication. The minimum length of a secret key is 8 characters and maximum 40 characters. Setting up secret keys does not initiate DH-CHAP authentication. If switch is configured to do DH-CHAP, it is performed whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

```
Press enter to start setting up secrets >
Enter WWN, Domain, or switch name (Leave blank when done): 10:00:00:60:69:80:05:14
Enter peer secret:
Re-enter peer secret:
Enter local secret:
Re-enter local secret:
Enter WWN, Domain, or switch name (Leave blank when done):
Are you done? (yes, y, no, n): [no] y
Saving data to key store... Done.
```

To view a DH-CHAP secret word database:

1. Log in as admin to the 400 MP Router, or 4/256 SAN Director or DC Director with an FR4-18i blade. At the Telnet prompt, enter the secAuthSecret command as shown:

```
switch:admin> secauthsecret --show
```

```
<table>
<thead>
<tr>
<th>WWN</th>
<th>DIId</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00:00:60:69:80:05:14</td>
<td>1</td>
<td>switch</td>
</tr>
</tbody>
</table>
```

For details about the setAuthSecret command, see the Fabric OS Command Reference.

**Configuring an interfabric link**

Before configuring an IFL, be aware that you cannot configure both IFLs (EX_Ports, VEX_Ports) and ISLs (E_Ports) from a backbone fabric consisting of a single 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade to the same edge fabric.

Configuring an interfabric link involves disabling ports and cabling them to other fabrics, configuring those ports for their intended use, and then enabling the ports.

When it is in strict mode, ACL cannot support Fibre Channel routing in the fabric. Before connecting an edge fabric to an FC router and before setting up the FC router in the BB, verify that the Fabric Wide Consistency Policy is not in 'strict' mode by issuing the fddCfg --showall command.

If the Fabric Wide Consistency Policy has the ‘S’ letter in it in the edge fabric or the BB fabric, do not connect the edge fabric or the BB to the FC router.

**NOTE:** To ensure that fabrics remain isolated, disable the port prior to inserting the cable. If you are configuring an EX_Port, disable the port prior to making the connection.
To configure an IFL for both edge and backbone connections:

1. On the 400 MP Router, or 4/256 SAN Director or DC Director with an FR4-18i blade, disable the port that you are configuring as an EX_Port (the one connected to the Brocade switch) by issuing the `portDisable` command.

   ```
   switch:admin> portdisable 7/10
   ```

   You can verify that port 7 has been disabled by issuing the `portShow` command for the port.

2. Configure each port that connects to an edge fabric as an EX_Port or VEX_Port. Note the following:
   - `portCfgVEXPort` works only on GbE ports.
   - `portCfgEXPort` (only on the FC ports on the 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade) commands work only on ports that are capable of FC-FC routing.

   Use the `portCfgEXPort` or `portCfgVEXPort` command to:
   - Enable or disable EX_Port or VEX_Port mode.
   - Set the fabric ID (avoid using fabric ID 1, which is the default for backbone connections).

   ```
   NOTE:  If an edge fabric with redundant links to the backbone fabric is segmented, hosts may lose connectivity to imported targets.
   ```

   Repair the edge fabric, then use the `portCfgEXPort` command to disable all EX_Ports to the edge fabric, and enable the EX_Ports again to restore connectivity.

   ```
   The following example enables the EX_Port (or VEX_Port) and assigns a Fabric ID of 30 to port 7.
   ```

   ```
   switch:admin> portcfgexport 7/10 -a 1 -f 30
   switch:admin> portcfgexport 7/10
   Port  7/10  info
   Admin:                  enabled
   State:                  NOT OK
   Pid format:             Not Applicable
   Operate mode:           Brocade Native
   Edge Fabric ID:         30
   Preferred Domain ID:    160
   Front WWN:              50:06:06:9e:20:38:6e:1e
   Fabric Parameters:      Auto Negotiate
   R_A_TOV:                Not Applicable
   R_D_TOV:                Not Applicable
   Authentication Type: None
   DH Group: N/A
   Hash Algorithm: N/A
   Edge fabric's primary wnn: N/A
   Edge fabric's version stamp: N/A
   ```
portCfgExport options

This port can now connect to another switch. The following list describes the options for the portCfgExport command. For more information about the portCfgExport and portCfgVexport commands, see the Fabric OS Command Reference.

- **-a**  
  Sets the EX_Port to enabled (1) or disabled (2). Admin use only.

- **-f**  
  Sets the fabric ID (1 to 128). Each edge fabric must have a unique ID, and EX_Ports (or VEX_Ports) connected to the same edge fabric must have the same fabric ID. The default value is the port number divided by 3, plus 2 and rounded down.

- **-r**  
  Sets the R_A_TOV used for port negotiation (2000 - 120000).

- **-e**  
  Sets the E_D_TOV used for port negotiation (1000 - 60000).

- **-d**  
  Preferred front Domain ID (1-239). This command enforces the use of the same preferred front Domain ID for all the ports connected to the same edge fabric.

  When this option is specified, the preferred front Domain ID is compared against the online ports. If the preferred front Domain ID is different, an error message is issued and the command fails.

  When the -d option is not specified, if there are online ports connected to the same edge fabric, the preferred front Domain ID is set to the preferred front Domain ID of those online ports. Otherwise, if there are offline ports that are set to EX_Port, the preferred front Domain ID is set to those offline ports. If none of the above conditions apply, the existing value is left untouched.

- **-p**  
  Sets the PID format (0-native, 1-core, 2-extended-edge). The value must match the edge fabric setting. The default value is 1.

- **-t**  
  Sets the negotiate fabric parameters (1-enable, 2-disable)

- **-m**  
  Sets the port mode. (0-Brocade, 1-Open, 2-McDATA Fabric, 3-McDATA Fabric Legacy). This command enforces the use of the same port mode for all the ports connected to the same edge fabric.

  When this option is specified, the port mode is compared against the online ports. If the modes are different, an error message is issued and the command fails.

  When the -m option is not specified:

  If there are online ports connected to the same edge fabric, the mode is set to the mode of those online ports. Otherwise, if there are offline ports that are set to EX_Port, the mode is set to those offline ports.

  If none of the above conditions apply, the existing value is left untouched.

For related FC-FC Routing commands, see fcrXlateconfig, fcrConfigure, and fcrProxyconfig in the Fabric OS Command Reference.

A Fibre Channel router can interconnect multiple fabrics. EX_Ports or VEX_Ports attached to more than one edge fabric must configure a different fabric ID for each edge fabric.

At this point you have some options to consider before proceeding to the next step. These options include FCR router port cost operations and setting up either ISL or EX_Port trunking. For information about using FCR Router Port Cost operations, see “Configuring the FC Router port cost (optional)” on page 230 and for information on trunking setup, see “Using EX_Port frame trunking” on page 234.

3. Enter the **portEnable** command to enable the ports that you disabled in step 2. You can now physically attach ISLs from the Fibre Channel Router to the edge fabric.

  switch:admin> portenable 7/10
4. Enter the `portCfgShow` command to view ports that are persistently disabled.

```
switch:admin> portcfgshow 7/10
Area Number:      74
Speed Level:      AUTO
Trunk Port        OFF
Long Distance     OFF
VC Link Init      OFF
Locked L_Port     OFF
Locked G_Port     OFF
Disabled E_Port   OFF
ISL R_RDY Mode    OFF
RSCN Suppressed   OFF
Persistent Disable OFF
NPIV capability   ON
EX Port           ON
Mirror Port       ON
FC Fastwrite      ON
```

5. After identifying such ports, enter the `portCfgPersistentEnable` command to enable the port, and then the `portCfgShow` command to verify the port is enabled.

```
switch:admin> portcfgpersistentenable 7/10

switch:admin> portcfgshow 7/10
Area Number:      74
Speed Level:      AUTO
Trunk Port        OFF
Long Distance     OFF
VC Link Init      OFF
Locked L_Port     OFF
Locked G_Port     OFF
Disabled E_Port   OFF
ISL R_RDY Mode    OFF
RSCN Suppressed   OFF
Persistent Disable OFF
NPIV capability   ON
EX Port           ON
Mirror Port       ON
FC Fastwrite      ON
```
6. Enter either the `portCfgEXPort` or `portShow` command to verify that each port is configured correctly:

```
switch:admin> portcfgexport 7/10
```

```
Port  7/10  info
Admin:          enabled  
State:          NOT OK  
Pid format:     Not Applicable  
Operate mode:   Brocade Native  
Edge Fabric ID:  30  
Preferred Domain ID:  160  
Front WWN:      50:06:06:9e:20:38:6e:1e  
Fabric Parameters:  Auto Negotiate  
R_A_TOV:       Not Applicable  
E_D_TOV:       Not Applicable  
Authentication Type: None  
DH Group:       N/A  
Hash Algorithm: N/A  
Edge fabric's primary wwn: N/A  
Edge fabric's version stamp: N/A  
```

```
switch:admin_06> portshow 7/10
```

```
portName:  
portHealth: OFFLINE  
Authentication: None  
EX_Port Mode: Enabled  
Fabric ID: 30  
Front Phantom: state = Not OK  
Pref Dom ID: 160  
Fabric params: R_A_TOV: 0  
E_D_TOV: 0  
PID fmt: au to
```

```
portDisableReason: None  
portCFlags: 0x1  
portFlags: 0x1  
PRESENT U_PORT EX_PORT  
portType: 10.0  
portState: 2  
Offline  
portPhys: 2  
No_Module  
portScn: 0  
port generation number: 0  
portId: 014a00  
portIfId: 4372080f  
portWwn: 20:4a:00:60:69:e2:03:86  
portWwn of device(s) connected:  
Distance: normal  
portSpeed: N4Gbps  
LE domain: 0  
FC Fastwrite: ON  
Interrupts: 0  
Link_failure: 0  
Frjt : 0  
Unknown: 0  
Loss_of_sync: 0  
Pbsy : 0  
Lli: 0  
Loss_of_sig: 2
```
**Proc_rqrd:** 0  **Protocol_err:** 0
**Timed_out:** 0  **Invalid_word:** 0
**Rx_flushed:** 0  **Invalid_crc:** 0
**Tx_unavail:** 0  **Delim_err:** 0
**Free_buffer:** 0  **Address_err:** 0
**Overrun:** 0  **Lr_in:** 0
**Suspended:** 0  **Lr_out:** 0
**Parity_err:** 0  **Ols_in:** 0
**2_parity_err:** 0  **Ols_out:** 0
**CMI_bus_err:** 0

Port part of other ADs: No

7. Enter the `switchShow` command to verify the EX_Port (or VEX_Port), edge fabric ID, and name of the edge fabric switch (containing the E_Port or VE_Port).

8. Enter the `fcrFabricShow` command to view any edge fabric’s switch names and ensure links are working as expected:

![NOTE: The `fcrFabricShow` command displays the static IPv6 addresses for each FC router and each edge fabric switch connected to the EX_Ports.]

```
switch:admin> fcrfabricshow
FCR WWN: 10:00:00:05:1e:13:59:00, Dom ID: 2, Info: 10.32.156.52
1080::8:800:200C:1234/64, "fcr_7500"
EX_Port PID Neighbor Switch Info (WWN, enet IP, name)
---------------------------------------------------------------
7 10 10:00:00:05:1e:34:11:e5 10.32.156.33 "7500" 1080::8:8FF:FE0C:417A/64
4 116 10:00:00:05:1e:37:00:44 10.32.156.34 "7500"
FCR WWN: 10:00:00:05:1e:12:e0:00, Dom ID: 100, Info:10.32.156.50
1080::8:60F:FE0C:456A/64
"fcr_7500"
EX_Port PID Neighbor Switch Info (WWN, enet IP, name)
------------------------------------------------------------------------
4 95 10:00:00:05:1e:37:00:45 10.32.156.31 "7500"
FCR WWN: 10:00:00:05:1e:12:e0:00, Dom ID: 100, Info:10.32.156.50, "fcr_Brocade 7500"
EX_Port PID Neighbor Switch Info (WWN, enet IP, name)
------------------------------------------------------------------------
4 95 10:00:00:05:1e:37:00:45 10.32.156.31 "Brocade 7500"
5 95 10:00:00:05:1e:37:00:45 10.32.156.31 "Brocade 7500"
6 95 10:00:00:05:1e:37:00:45 10.32.156.31 "Brocade 7500"
```

**Configuring the FC router port cost (optional)**

FC routers optimize the usage of the router port links by directing traffic to the link with the smallest router port cost. The FC router port cost is similar to the link cost setting available on E_Ports, which allows you to customize traffic flow. The router port link cost values are either 1000 or 10,000. The router module chooses the router port path based on the lowest cost per FID connection. If multiple paths exist where one path costs lower than the others, then the lowest cost path is used. If exchange-based routing has not been disabled and multiple paths exist with the same lowest cost, there will be load sharing over these paths.

Implementing the router port cost feature optimizes the usage of the router port links by directing the traffic to a link with a smaller cost. For example, if there are EX_ and VEX_Port connections to the same edge fabric, the traffic will be directed through the EX_Port link.

Every IFL has a default cost. The default router port cost values are:

- 1000 for legacy (v5.1 or XPath FCR) IFL
- 1000 for EX_Port IFL
- 10,000 for VEX_Port IFL
The FCR router port cost settings are 0, 1000, or 10,000. If the cost is set to 0, the default cost will be used for that IFL. The FC router port cost is persistent and is saved in the existing port configuration file.

Router port cost is passed to other routers in the same backbone. Link costs from the front domain to the translate (xlate) domain remain at 10,000. You can use the `lsDbShow` from the edge fabric to display these link costs.

### Using router port cost

Initially, the router port cost value for an EX_Port is set automatically when the EX_Port is created with the `portCfgExport` command. However, you can use the `fcrRouterPortCost` to modify the cost for that port. You can configure the EX_ or VEX_Port with either 1000 or 10,000 values. If you wish to differentiate between two EX_Port links with different speeds, you can assign 1000 to one link and 10,000 to the other link.

For details about the use of any of the following commands, see the Fabric OS Command Reference.

To make any changes to an EX_ and VEX_Port, the `-a` admin option must be enabled using the `portCfgExport` or `portCfgVexport` command. However, to make changes to the router port cost, the port must be disabled using `portdisable`.

To set the cost of an EX_Port:

```bash
switch:admin> fcrrouterportcost 7/10 10000
```

To set and display the router port cost:

1. Disable any port on which you want to set the router port cost.
2. Enable admin for the EX_Port or VEX_Port with `portCfgExport` or `portCfgVexport` command.
3. Enter the `fcrRouterPortCost` command to display the router port cost per EX_Port.

```bash
switch:admin> fcrrouterportcost
Port             Cost
------------------------
7/3              1000
7/4              1000
7/9              1000
7/10             1000
7/13             1000
10/0             1000
```

You can also use the `fcrRouteShow` command to display the router port cost.

4. Enter the `fcrRouterPortCost` command with a port and slot number, to display the router port cost for a single EX_Port.

```bash
switch:admin_06> fcrrouterportcost 7/10
Port             Cost
------------------------
7/10             1000
```

5. Enter the `fcrRouterPortCost` command with a port and slot number and a specific cost, to set the router port cost for a single EX_Port.

```bash
switch:admin_06> fcrrouterportcost 7/10 10000
```

6. Enter the `fcrRouterPortCost` command, to set the cost of the EX_Port back to the default.

```bash
switch:admin_06> fcrrouterportcost 7/10 0
```

### Upgrade, downgrade, and HA considerations

- For HA, the router port cost is synchronized to the standby CP.
- Legacy routers in the backbone fabric program all the router ports without considering router port cost. Fabric OS 5.2.0 or later considers the legacy router port cost as 1000 for both EX or VEX_Ports.
Port cost considerations

The router port cost has the following considerations:

- Router port sets are defined as follows:
  - 0-7 and FCIP Tunnel 16-23
  - 8-15 and FCIP Tunnel 24-31

More than two router port sets can exist in a 4/256 SAN Director or DC Director with two FR4-18i blades.

- The router port cost does not help distinguish one IFL (or EX_ and VEX_Port link) from another, if all the IFLs are connected to the same port set. Therefore, if you connect IFL1 and IFL2 to the same edge fabric in port set 0–7 and then configure them to different router port costs, traffic is still balanced across all the IFLs in the same port set.

- Use proper SAN design guidelines to connect the IFLs to different port sets for effective router port cost use. For example, if both a low-speed VEX_Port and a high-speed EX_Port are going to the same edge fabric, connect the lower router cost IFLs to a separate port group (for example ports 0–7) than the higher router cost IFLs (for example ports 8–15). For VEX_Ports, you would use ports in the range of 16-23 or 24-31.

You can connect multiple EX_Ports or VEX_Ports to the same edge fabric. The EX_Ports can all be on the same 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade, or they can be on multiple routers. Multiple EX_Ports create multiple paths for frame routing. Multiple paths can be used in two different, but compatible, ways:

- Failing over from one path to another.
- Using multiple paths in parallel to increase effective data transmission rates.

EX_Ports and VEX_Ports, when connected, are assigned different router port costs and traffic will flow only through the EX_Ports. Routing failover is automatic, but it can result in frames arriving out of order when frames take different routes. The 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade can force in-order delivery, although frame delivery is delayed immediately after the path failover.

Source EX_Ports can balance loads across multiple destination EX_Ports attached to the same edge fabric using exchange IDs from the routed frames as keys to distribute the traffic.

Setting a proxy PID

When a 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade is first configured, the PIDs for the proxy devices are automatically assigned. Proxy PIDs (as well as phantom Domain IDs) persist across reboots.

The most common situation in which you would set a proxy PID is when you replace a switch. If you replace the switch and want to continue using the old PID assignments, you can configure it to do so; this value remains in the system even if the blade is replaced. To minimize disruption to the edge fabrics, set the proxy PIDs to the same values used with the old hardware.

The `fcrProxyConfig` command displays or sets the persistent configuration of proxy devices. Used with the `-s slot` option, it can also influence the assignment of the xlate domain port number (which is used to determine the Area_ID field of the PID) and the Port_ID field. Like the PIDs in a fabric, a proxy PID must be unique. If the slot argument results in a duplicate PID, it will be ignored. Proxy PIDs are automatically assigned to devices imported into a fabric, starting at f001. For Proxy IDs projected to a McDATA edge fabric in McDATA fabric mode, use valid ALPAs (lower 8 bits). See the `fcrProxyConfig` command in the Fabric OS Command Reference for more details.

Use the `fcrXlateConfig` command to display or assign a preferred Domain ID to a translate domain. See the Fabric OS Command Reference for more details.

Matching fabric parameters

By default, EX_Ports and VEX_Ports detect, autonegotiate, and configure the fabric parameters without user intervention.

You can optionally configure these parameters manually. To change the fabric parameters on a switch in the edge fabric, execute the `configure` command. To change the fabric parameters of an EX_Port on the
400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade, use the portCfgEXPort command. If you want to change the fabric parameters of a VEX_Port, then use the portCfgVEXPort command.

The PID mode for the backbone fabric PID mode and the edge fabric PID mode do not need to match, but the PID mode for the EX_Port or VEX_Port and the edge fabric to which it is attached must match. You can statically set the PID mode for the fabric by using the \(-p\) option with the portCfgEXPort command. (Use the \(-E\) option to disable the negotiate fabric parameter feature). Otherwise, the PID mode is autonegotiated. The various edge fabrics may have different PID modes.

Fabric parameter settings, namely, E_D_TOV (error-detect timeout value), R_A_TOV (resource-allocation timeout value), and PID format, must be the same on EX_Ports or VEX_Ports and on the fabrics to which they are connected. You can set the PID format on an EX_Port when you configure an interfabric link.

The default values for E_D_TOV and R_A_TOV for an EX_Port or VEX_Port must match those values on other HP switches. Only if you have adjusted these parameters for the edge fabric do you need to adjust them for an EX_Port or VEX_Port.

The default values for R_A_TOV and E_D_TOV are the recommended values for all but very large fabrics (ones requiring four or more hops) or high-latency fabrics (such as ones using long-distance FCIP links).

**Configuring EX_Port frame trunking (optional)**

In Fabric OS 5.2.0 and later, you can configure EX_Ports to use frame based trunking just as you do regular E_Ports. EX_Port frame trunking support is designed to provide the best utilization and balance of frames transmitted on each link between the FCR and the edge fabric. You should trunk all ports connected to the same edge fabrics.

The FC router front domain has a higher node WWN—derived from the FC router—than that of the edge fabric. Therefore, the FCR front domain initiates the trunking protocol on the EX_Port.

After initiation, the first port from the trunk group that comes online is designated as the master port. The other ports that come online on the trunk group are considered the slave ports. Adding or removing a slave port does not cause frame drop.

The restrictions for EX_Port frame trunking are the same as for E_Ports—all the ports must be adjacent to each other using the clearly marked groups on the front of the product.

EX_Port frame-based trunking has a master trunk link. If the master trunk link goes down, the entire EX_PORT-based trunk will reform and it will be taken offline for a short period of time. If there are no other links to the edge fabric from the backbone, the master port going offline may cause a traffic disruption in the backbone.

**IMPORTANT:** Fabric OS 5.2.0 introduces the EX_Port trunking feature. This feature should only be enabled if the entire configuration is running Fabric OS 5.2.0 and later. Enabling the EX_Port trunking feature on a switch running Fabric OS 5.2.0 or later in a configuration containing a Fabric OS 5.1.0 switch will cause the Fabric OS 5.1.0 switch to panic.

If router port cost is used with EX_Port trunking, the master port and slave ports share the router port cost of the master port.

For information about setting up E_Port trunking on an edge fabric, see “Administering ISL Trunking” on page 129 in this guide.
Supported configurations and platforms

The EX_Port trunking is an FCR software feature and requires that you have a trunking license installed on the FCR switch and on the edge fabric connected to the other side of the trunked EX_Ports. EX_Port trunking is supported only with edge fabrics. You can use EX_Port frame trunking in the following configurations and cases:

- Ports with speeds of 2 Gbps up to a maximum speed of 4 Gbps and trunking over long distance.
- In the edge fabric, when FCR is connected to a Condor-based switch such as the SAN Switch 4/32, SAN Switch 4/32B, 4/64 SAN Switch, 4/256 SAN Director or DC Director with an FC4-48 blade, that supports eight ports from the trunkable group.
- When FCR is connected to Bloom-based switches, such as the SAN Switch 2/16, SAN Switch 2/32, SAN Director 2/128, or FC-16 blade, supporting four ports in the trunk group. If the edge fabric is a Bloom-based switch, the FCR will set up the trunking for four ports per trunk.
- When FCR is connected to an edge fabric using a mix of trunked and non-trunked EX_Ports. All will share the same front domain.
- With a Secure Fabric OS edge fabric.

High Availability support

The EX_Port frame trunking feature also is a High Availability (HA) supported feature. The HA protocol for EX_Port trunking is as follows:

- If trunking is disabled prior to the HA failover, it remains disabled after the HA failover.
- If trunking is enabled prior to the HA failover, it remains enabled after the HA failover.

Backward compatibility support

For backward compatibility, FCR that supports EX_Port trunking can continue to interoperate with older FCR switches and all previously supported Brocade switches in the Brocade edge fabric.

Using EX_Port frame trunking

With EX_Port frame trunking, you can use the same CLI commands as you do for E_Port trunking.

Security considerations

Administration control for EX_Port trunking is available through root, admin, and switch admin access.

Trunking commands

The procedure for administering EX_Port frame trunking is the same as for E_Port trunking. You initialize trunking on ports with portCfgTrunkPort or switchCfgTrunk, and monitor traffic with the portPerfShow command. You need a Brocade license to enable trunking; however, you can disable trunking on the ports without the trunking license installed. You can use the following commands to enable and disable trunking:

- Disable (0) or enable (1) trunking on a single port using the portCfgTrunkPort command. The following example shows how to disable trunking on a single port and then how to enable trunking.

  switch:admin_06> portcfgtrunkport 1/10 0

  switch:admin_06> portcfgtrunkport 1/10 1

- Disable (0) or enable (1) trunking on all the ports of a switch using the switchCfgTrunk command. The following example shows how to disable trunking on all ports and then how to enable trunking.

  switch:admin_06> switchcfgtrunk 0

  switch:admin_06> switchcfgtrunk 1

  Configuration applied to all ports except the following VE/VEX_Ports (ports 128 - 143, 192 - 207).

  When either command is executed to update the trunking configuration, the ports for which the configuration applies are disabled and re-enabled with the new trunk configuration. As a result, the traffic...
through these ports may be disrupted for a short period of time. In addition to the commands for enabling and disabling trunking, you can also use the following E_Port commands for administering EX_Port Frame Trunking:

- Use `portCfgSpeed` and `switchCfgSpeed` to set speed for a port or switch.
- Display lists of trunks and members of trunks with the `trunkShow` command.
- Use `trunkDebug` to list link characteristics for troubleshooting.
- Use the `switchShow` command to display the trunking information on the EX_Ports.

For details about using these commands, see “Administering ISL Trunking” on page 129 and individual commands in the Fabric OS Command Reference.

To display EX_Port trunking information:

1. Log in as an admin and connect to the switch.
2. Enter the `switchShow` command to display trunking information for the EX_Ports.

```
fcr_switch:admin> switchshow
The following is an example of a master EX_Port and a slave EX_Port displayed in switchShow.
Index Slot Port Address Media Speed State
==============================================
16  2  0  ee1000  id  N4  No_Light
17  2  1  ee1100  id  N4  Online  EX_Port  (Trunk port, master is Slot 2 Port 2 )
18  2  2  ee1200  id  N4  Online  EX_Port  "MtOlympus_82" (fabric id = 2 ) (Trunk master)
19  2  3  ee1300  id  N4  No_Light
20  2  4  ee1400  id  N4  Online  EX_Port  (Trunk port, master is Slot 2 Port 7 )
21  2  5  ee1500  id  N4  Online  EX_Port  (Trunk port, master is Slot 2 Port 7 )
22  2  6  ee1600  id  N4  Online  EX_Port  (Trunk port, master is Slot 2 Port 7 )
23  2  7  ee1700  id  N4  Online  EX_Port  "MtOlympus_72" (fabric id = 2 ) (Trunk master)
```

To display trunking information for a switch:

- Use the `trunkShow` command to display trunking information for a switch.

```
switch:admin> trunkshow
1: 6 ->  4  10:00:00:60:69:51:43:04  deskew 15  MASTER
2:15 -> 13  10:00:00:60:69:51:43:04  deskew 16  MASTER
12 -> 12  10:00:00:60:69:51:43:04  deskew 15
14 -> 14  10:00:00:60:69:51:43:04  deskew 17
13 -> 15  10:00:00:60:69:51:43:04  deskew 16
3:24 -> 14  10:00:00:60:69:51:42:dd  deskew 15  MASTER
```

Configuring LSANs and zoning

An LSAN consists of zones in two or more edge or backbone fabrics that contain the same devices. LSANs essentially provide selective device connectivity between fabrics without forcing you to merge those fabrics. FC routers provide multiple mechanisms to manage interfabric device connectivity through extensions to existing switch management interfaces. You can define and manage LSANs using Advanced Zoning or Fabric Manager.

Use of administrative domains with LSAN zones and FCR

You can create LSAN zones as a physical fabric administrator or as an individual administrative domain (AD) administrator. The LSAN zone can be part of the root zone database or the AD zone database. FCR harvests the LSAN zones from all administrative domains. If both edge fabrics have the matching LSAN zones and both devices are online, FCR triggers a device import. To support legacy applications, WWNs are reported based on the administrative domain context. As a result, you must not use the network...
address authority (NAA) field in the WWN to detect an FC router. LSAN zone enforcement in the local fabric occurs only if the administration domain member list contains both of the devices (local and imported device) specified in the LSAN zone.

For more information, see “Managing administrative domains” on page 143.

Defining and naming zones

Zones are defined locally on a switch or director. Names and memberships, with the exception of hosts and targets exported from one fabric to another, do not need to be coordinated with other fabrics. For example, in Figure 10 on page 218, when the zones for Edge SAN 1 are defined, you do not need to consider the zones in Edge SAN 2, and vice versa.

Zones that contain hosts and targets that are shared between the two fabrics need to be explicitly coordinated. To share devices between any two fabrics, you must create an LSAN zone in both fabrics containing the port WWNs of the devices to be shared. Although an LSAN is managed using the same tools as any other zone on the edge fabric, two behaviors distinguish an LSAN from a conventional zone:

• A required naming convention. The name of an LSAN begins with the prefix “LSAN_”. The LSAN name is case-insensitive; for example, _lsan_ is equivalent to _LSAN_, _Lsan_, and so on.

• Members must be identified by their port WWN because port IDs are not necessarily unique across fabrics. The names of the zones need not be explicitly the same, and membership lists of the zones need not be in the same order.

To enable device sharing across multiple fabrics, you must create LSAN zones on the edge fabrics (and optionally on the backbone fabric, as well), using normal zoning operations to create zones with names that begin with the special prefix “LSAN_”, and adding host and target port WWNs from both local and remote fabrics to each local zone as desired. Zones on the backbone and on multiple edge fabrics that share a common set of devices will be recognized as constituting a single multi-fabric LSAN zone, and the devices that they have in common will be able to communicate with each other across fabric boundaries.

LSAN zones and fabric-to-fabric communications

Zoning is enforced by all involved fabrics, any communication from one fabric to another must be allowed by the zoning setup on both fabrics. If the SANs are under separate administrative control, then separate administrators maintain access control.

__NOTE:__ If you are managing other switches in a fabric, it is recommended that you run the `defZone --show` command on your Fabric OS 5.1.0 and later switches as a precaution. Default zoning behavior in Fabric OS 5.1.0 and later operates differently compared to earlier versions of Fabric OS (2.x, 3.x v4.x and 5.0.1).

For example, if you issue the `defZone --noaccess` command on a Fabric OS 5.1.0 or later switch, then default zoning configurations will be created on each switch in the fabric (2.x, 3.x, 4.x or v.0.1 switches). Fabric OS 5.1.0 and later switches do not indicate that a default configuration is enabled when you use the `cfgShow` or `cfgActvShow` commands. For more information about default zoning, refer to “Administering Advanced Zoning” on page 387.

The following example procedure illustrates how LSANs control which devices can communicate with each other. The example procedure shows the creation of two LSANs (called `lsan_zone_fabric75` and `lsan_zone_fabric2`), which involve the following devices:

• Switch1 and the host in fabric75.
• Switch2, Target A, and Target B in fabric2.
• Switch1 is connected to the 4/256 SAN Director or DC Director with an FR4-18i blade using an EX_Port or VEX_Port.
• Switch2 is connected to the 4/256 SAN Director or DC Director with an FR4-18i blade using another EX_Port or VEX_Port.
• Host has WWN 10:00:00:00:c9:2b:c9:0c (connected to switch1).
• Target A has WWN 50:05:07:61:00:5b:62:ed (connected to switch2).
• Target B has WWN 50:05:07:61:00:49:20:b4 (connected to switch2).

The following procedure shows how to control device communication with the LSAN.

To control device communication with the LSAN:

1. Log in as admin and connect to switch1.
2. Enter the nsShow command to list the WWN of the host (10:00:00:00:c9:2b:c9:0c).

**NOTE:** The nsShow output displays both the port WWN and node WWN; the port WWN must be used for LSANs.

```
switch:admin> nsShow
{
  Type  Pid         COS     PortName                NodeName                 TTL(sec)
  N       060f00; 2,3; 10:00:00:00:c9:2b:c9:0c; 20:00:00:00:c9:2b:c9:0c; na
    FC4s: FCP
    NodeSymb: [35] "Emulex LP9002 FV3.91A3 DV5-5.20A6"
    Fabric Port Name: 20:0f:00:05:1e:37:00:44
    Permanent Port Name: 10:00:00:00:c9:2b:c9:0c
    The Local Name Server has 1 entry }
3. Enter the zoneCreate command to create the LSAN lsan_zone_fabric75, which includes the host.
   switch:admin> zoneCreate "lsan_zone_fabric75", "10:00:00:00:c9:2b:c9:0c"
4. Enter the zoneAdd command to Target A to the LSAN.
   FID75Domain5:admin> zoneAdd "lsan_zone_fabric75", "50:05:07:61:00:5b:62:ed"
5. Enter the cfgAdd or cfgCreate and cfgEnable commands to add and enable the LSAN configuration.
   switch:admin> cfgAdd "zone_cfg", "lsan_zone_fabric75"
   switch:admin> cfgEnable "zone_cfg"
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the current configuration selected.
Do you want to enable 'zone_cfg' configuration (yes, y, no, n): [no] y
zone config "zone_cfg" is in effect
Updating flash ...
7. Enter the nsShow command to list Target A (50:05:07:61:00:5b:62:ed) and Target B (50:05:07:61:00:49:20:b4).
   switch:admin> nsShow
{
  Type  Pid         COS     PortName                NodeName                 TTL(sec)
  NL      0508e8; 3; 50:05:07:61:00:5b:62:ed; 50:05:07:61:00:1b:62:ed; na
    FC4s: FCP [IBM DNEP-309170 F90F]
    Fabric Port Name: 20:08:00:05:1e:34:11:e5
    Permanent Port Name: 50:05:07:61:00:5b:62:ed
  NL      0508ef; 3; 50:05:07:61:00:49:20:b4; 50:05:07:61:00:09:20:b4; na
    FC4s: FCP [IBM DNEP-309170 F90F]
    Fabric Port Name: 20:08:00:05:1e:34:11:e5
    Permanent Port Name: 50:05:07:61:00:49:20:b4
    The Local Name Server has 2 entries }
8. Enter the zoneCreate command to create the LSAN lsan_zone_fabric2, which includes the host (10:00:00:00:c9:2b:6a:2c), Target A, and Target B.
   switch:admin> zoneCreate "lsan_zone_fabric2",
   "10:00:00:00:c9:2b:c9:0c;50:05:07:61:00:5b:62:ed;50:05:07:61:00:49:20:b4"
9. Enter the `cfgShow` command to verify that the zones are correct.

```
switch:admin> cfgshow
Defined configuration:
  zone: lsan_zone_fabric2
    10:00:00:00:c9:2b:c9:0c; 50:05:07:61:00:5b:62:ed;
    50:05:07:61:00:49:20:b4
```

Effective configuration:
no configuration in effect

10. Enter the `cfgAdd` and `cfgEnable` commands to create and enable the LSAN configuration.

```
switch:admin> cfgadd "zone_cfg", "lsan_zone_fabric2"
switch:admin> cfgenable "zone_cfg"
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected.
Do you want to enable 'zone_cfg' configuration (yes, y, no, n): [no] y
zone config "zone_cfg" is in effect
Updating flash ...
```

11. Log in as an admin and connect to the 4/256 SAN Director or DC Director with a FR4-18i blade.

12. Enter the following commands to display information about the LSANs.

- `lsanZoneShow -s` shows the LSAN.

```
switch:admin> lsanzoneshow -s
Fabric ID: 2 Zone Name: lsan_zone_fabric2
  10:00:00:00:c9:2b:c9:0c  Imported
  50:05:07:61:00:5b:62:ed  EXIST
  50:05:07:61:00:49:20:b4  EXIST
Fabric ID: 75 Zone Name: lsan_zone_fabric75
  10:00:00:00:c9:2b:c9:0c  EXIST
  50:05:07:61:00:5b:62:ed  Imported
```

- `fcrPhyDevShow` shows the physical devices in the LSAN.

```
switch:admin> fcrphydevshow
Device           WWN            Physical
Exists                            PID
in Fabric                                   in Fabric
-----------------------------------------
75 10:00:00:00:c9:2b:c9:0c  c70000
  2 50:05:07:61:00:5b:62:ed  0100ef
  2 50:05:07:61:00:5b:62:ed  0100e8
Total devices displayed: 3
```

- `fcrProxyDevShow` shows the proxy devices in the LSAN.

```
switch:admin> fcrproxydevshow
Proxy           WWN             Proxy      Device   Physical    State
Created                           PID       Exists     PID       in Fabric
                                      in Fabric
----------------------------------------------------------------------------
75   50:05:07:61:00:5b:62:ed  01f001       2       0100e8   Imported
2    10:00:00:00:c9:2b:c9:0c  02f000       75      c70000   Imported
Total devices displayed: 2
```

On the 4/256 SAN Director or DC Director with an FR4-18i blade, the host and Target A are imported, because both are defined by `lsan_zone_fabric2` and `lsan_zone_fabric75`. However, target B defined by `lsan_zone_fabric75` is not imported because `lsan_zone_fabric2` does not allow it.

When a PLOGI, PDISC, or ADISC arrives at the 4/256 SAN Director or DC Directory with an FR4-18i blade, the SID and DID of the frame are checked. If they are LSAN-zoned at both SID and DID edge fabrics, the frame will be forwarded to the DID. If they are not zoned, only the PLOGI is dropped; for the remaining frames zoning enforcement takes place in the edge fabrics.
LSAN zone binding (optional)

By default, the Fibre Channel routers (FCR) in the backbone maintain the entire LSAN zone and device state database. On Fibre Channel routers with Fabric OS 5.3.0 and later, the LSAN zone binding allows you to specify pairs of edge fabrics that share devices, effectively creating an LSAN fabric matrix. The Fibre Channel router uses this information to store only the LSAN zone entries of the remote edge fabrics that can access its local edge fabrics and also to search and do a pair match only against the specified edge fabrics. The advantage is that an individual Fibre Channel router may store fewer LSAN zone entries, and the LSAN zone limit supported in the backbone will not be limited by the capability of one FCR. In addition, the pair match calculation that establishes the devices import/export states will consume less CPU time since the pair match will be done within the specified fabric boundaries and not against all the edge fabrics in the backbone. If you choose not to implement this feature, the LSAN zone retains its default behavior.

If you decide to implement LSAN zone binding, then the imported devices in the metaSAN are not limited by the 10,000 LSAN device entries. Due to the lower LSAN count, the CPU consumption by the Fibre Channel router will be lower. If you configure the metaSAN such that the backbone has two groups of FCRs and there are no LSAN zone sharing and devices access between the two groups, the number of Fibre Channel routers and devices supported in the backbone can be higher.

The command `fcrlsanmatrix` is used to specify pairs of edge fabric IDs that will share devices. Those edge fabrics will have access only to the edge fabrics associated with them using this command. This LSAN fabric matrix is saved persistently and referred to as static binding. The edge fabrics that were not specified will have access to the rest of the other edge fabrics that were not specified. This association of the edge fabric IDs is called default or dynamic binding, which is the default behavior. Using this information, the FCR switch will maintain the remote LSAN Zone and the device state database only if it is associated with its local edge fabrics.

**NOTE:** This feature is supported only in a fabric with Fabric OS 5.3.0 and later Fibre Channel routers in the backbone.

The `fcrlsanmatrix` command is local to a Fibre Channel router and its configuration data will be saved locally. The configuration is not distributed automatically to other Fibre Channel routers on the backbone. The `fcrlsanmatrix` command is used to configure each of the FCRs in the backbone that support this feature.

For example, if edge fabrics with IDs 1, 2, 3, 4, and 5 are online, the default behavior is that every edge fabric allows access to each other. If later on, FIDs 1 and 2 are specified to have exclusive access using the command `fcrlsanmatrix`, then:

- FID 1 can access only FID 2.
- FID 2 can access only FID 1.
- FIDs 3, 4, and 5 can access each other but cannot access FIDs 1 or 2.

The FIDs entered do not need to be online when setting up the LSAN fabric matrix. The LSAN fabric matrix information is saved per Fibre Channel router and not distributed to other FCRs automatically. The best practice is to enter the same information for all the Fibre Channel routers in the backbone that support this command.

The `fcrlsanmatrix` command is explained in detail below:

```
command with no option Displays the matrix information that is saved in the persistent memory.
FabricID1 FabricID2 Specifies the fabric ID of the two edge fabrics that will be paired.
--add Adds the pair of FIDs to the cache.
--remove Removes the pair of FIDs from the cache.
--apply Applies the changes from the cache to persistent memory.
```
NOTE: The command fcrlsanmatrix --add 0 0 will erase the entire LSAN Zone Matrix settings in the cache.

To set up LSAN zone binding:
1. Log in to the switch as admin.
2. Enter the following command to add a pair:
   
   FCR:Admin > fcrlsanmatrix --add <FabricID1> <FabricID2>
3. Enter the following command to apply the changes persistently:
   
   FCR:Admin > fcrlsanmatrix --apply

To view the LSAN zones static and dynamic bindings:
1. Log on to the switch as admin.
2. Enter the command as follows:
   
   fcrlsanmatrix --fabricview

   The following is an example:
   
   FCR:Admin > fcrlsanmatrix --fabricview
   LSAN MATRIX is activated

<table>
<thead>
<tr>
<th>Fabric ID 1</th>
<th>Fabric ID 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>10</td>
<td>19</td>
</tr>
</tbody>
</table>

   Default LSAN Matrix:
   1 2 8

   See the Fabric OS Command Reference Manual for additional information on the fcrlsanmatrix command.

Dual backbone configuration

When dual backbones share edge fabrics, one of the backbones is selected to be the owner of the edge fabric which sends device state updates to the other backbone through the shared edge fabric. When the 'LSAN Zone binding' feature is enabled, the LSAN Zone Matrix settings for the shared edge fabrics must be the same on both backbones. Both backbone fabrics must have the same LSAN Zone Matrix settings.

If the settings are different, the outcome will be inconsistent. Both backbone fabrics will end up having the setup of the owner fabric which can change on reboot or on a port disable or enable.

Maximum LSAN count

The fcrlsancount command lets you configure the maximum number of LSANs, or LSAN count, that can be configured on the edge fabric, which is up to 5000 without disabling the switch. By default, the maximum LSAN count is set to 3000. This command lets you create more LSANs on your edge fabric where needed. The maximum number of devices supported is still 10000.
The `fcrlsancount` command assumes that all the FCRs in the same LSAN fabric matrix or backbone have the same maximum LSAN count defined, to protect all the FCRs from running into indefinite state. Asymmetric LSAN configurations due to different maximum LSAN counts could lead to different devices being imported on different FCRs.

The following example shows the use of the `fcrlsancount` command that allows you to display the current LSAN limit or to set the maximum LSAN Zone count:

To display the current LSAN limit:
```
switch:admin> fcrlsancount
LSAN Zone Limit 3000
```
To set the new LSAN zone limit:
```
switch:admin> fcrlsancount 5000
LSAN Zone Limit 5000
```

For information on how to display the new maximum LSAN count after it has been changed, see “Monitoring resources” on page 242.

**NOTE:** Since the maximum number of LSANs is configured per switch, if there is a different maximum LSAN count on the switches throughout the metaSAN, then the device import/export will not be identical on the FCRs. You should enter the same maximum LSAN count for all the FCR switches in the same backbone that support this feature. Verify the configured maximum limit against the LSANs configured using the `fcrresourceshow` command.

### Configuring backbone fabrics for interconnectivity

If you want devices in backbone fabrics to communicate with devices in edge fabrics, follow the steps in the section “To set up LSAN zone binding:” on page 240. However, instead of configuring the LSAN in the second edge fabric, configure the LSAN in the backbone fabric.

### HA and downgrade considerations

- The LSAN zone matrix is synchronized to the standby CP.
- On a dual CP switch, both CPs need to have the 5.3.0 code or later to enable the feature.
- If the feature is enabled on the active CP, introducing a CP with an earlier version of Fabric OS as a standby will fail the HA synchronization.
- If the feature is enabled, before downgrading to an earlier Fabric OS version, you will be asked to go back to the default mode.
- This feature does not have any impact on current HA functionality. LSANs will be synchronized as usual after the limit is increased and new LSANs are created.

### IPFC over FCR

IPFC over FCR supports IP device communication between edge-to-edge fabrics and edge-to-backbone fabrics. For IPFC over FCR to work, the FC router must be able to receive and forward broadcast frames from edge and backbone fabrics. To route broadcast frames to edge fabrics or the backbone fabric, FCR maintains a link state database (LSDB) and broadcast tree per edge fabric. The LSDB is a database that contains link state records (LSR) of all the switches in edge fabrics. Using data from the LSDB, the FC router constructs a broadcast tree and routes the frame to the destination using the shortest path of the broadcast tree. The IPFC over FCR feature does not require any additional licensing.

If switches in edge fabrics and the backbone fabric have Fabric OS v5.3.0 and later, a broadcast zone must be configured to share IP devices. Only devices in the broadcast zone will be able to receive broadcast frames. Broadcast zoning is supported only in 5.3.0 and later.

In 5.1.x and 5.2.x where broadcast zones are not implemented, all devices will be able to receive the broadcast packet. If it is required to set up a broadcast zone, the broadcast zone must include the IP device that exists in that edge or backbone fabric and the proxy device of the remote IP device.
In the FC router, use the command `fcrbcastconfig` to prevent interfabric forwarding of broadcast frames of edge or backbone fabrics.

Using the `fcrbcastconfig` command, you can disable or enable the broadcast frame forwarding option per FID (edge fabric or backbone fabric).

If you have an FID with a pre-existing IPFC data session that you want to disable then the IPFC traffic across the FCR may not stop even after disabling the broadcasting to some edge fabrics. When you disable the IPFC traffic broadcast configuration it will take effect on the next ARP command. If there is an active IPFC data session through the FCR, disabling the FID on the FCR, using the `fcrbcastconfig` command, would be effective after clearing the ARP cache on the host of the IP devices forcing the IP devices to re-send ARP or after the IP devices send the periodic ARP command. Clearing the ARP cache forces the IP devices to re-send ARP or after the IP devices send the periodic ARP command.

**Broadcast configuration**

To enable broadcast frames across the FC router, the IP devices must be LSAN-zoned. By default, the edge fabrics and the backbone fabric of the FC router have the broadcast frame receiving and forwarding option enabled. Users with Admin and switchAdmin roles can change the broadcast configuration using the `fcrbcastconfig` command. Thus multi-protocol devices can be configured to send broadcast frames to edge fabrics but not to others. For example, broadcast frames can be routed or prevent routing from edge-to-edge, backbone-to-edge, and edge-to-backbone fabrics.

Broadcast zoning can be used in an edge fabric to share IP devices. Only edge fabrics in the broadcast zone will be able to receive broadcast frames. In v5.1.x and v5.2.x where broadcast zones are not implemented, all the devices will be able to receive the broadcast packet. You can use the `fcrbcastconfig` command to set edge fabrics to receive broadcast frames. On switches with an earlier Fabric OS version than v5.3.0 that do not support broadcast zoning, the `fcrbcastconfig` command sets up inter-fabric broadcast frame forwarding on the FC router and prevents inter-fabric forwarding of broadcast frames to the switches running older versions of firmware.

Between FC routers, the broadcast frame is sent through the FC router protocol frame. The `fcrbcastconfig` command allows you to configure VEX_ and EX_Ports to enable or disable broadcast capability. The device that originates the broadcast frame must be imported in order to broadcast over FC routers.

**NOTE:** `fcrbcastconfig` configuration information does not propagate to other FCRs in the backbone fabric. If you configure one FCR you must configure all the FCRs with same configuration information across all FCRs in the fabrics.

To display the current broadcast zone configuration:

1. Log in to the switch as admin.
2. Type the following command:
   ```
   fcr:admin> fcrbcastconfig --show
   ```

   This command displays only the FIDs that have the broadcast frame option disabled. The FIDs that are not listed have the broadcast frame option enabled.

To enable the broadcast frame forwarding:

1. Log in to the switch as admin.
2. Type the following command:
   ```
   fcr:admin> fcrbcastconfig --enable -f <fabric id>
   ```

   where `<fabric id>` is the specified FID where you want to enable frame forwarding. This feature is turned on by default. This command enables the broadcast frame forwarding option for an FID (edge or backbone fabric).

To disable a broadcast zone forwarding:

1. Log in to the switch as admin.
2. Type the following command:

```
fcr:admin> fcrbcastconfig --disable -f <fabric id>
```

where `<fabric id>` is the specified FID where you want to disable frame forwarding. This command disables the broadcast frame forwarding option for an FID (edge or backbone fabric).

**Monitoring resources**

It is possible to exhaust resources, such as proxy PIDs. Whenever a resource is exhausted, Fabric OS generates an error message. The messages are described in the *Fabric OS Message Reference*.

You can monitor 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade resources using the `fcrResourceShow` command. The `fcrResourceShow` command shows FCR resource limits and usage and includes:

- LSAN zones and LSAN devices—The information shows the maximum versus the currently used zones and device database entry. LSAN is the count of LSANs in all the edge fabrics. If they are defined in two edge fabrics, they are counted as two and not one. One device imported into multiple edge fabrics counts multiple times. In Fabric OS 5.3.0 and later, you can have 3,000 LSAN zones configurable up to a maximum of 5,000. On a dual CP switch, both CPs must have v5.3.0 code or later to select 5000. If the active CP is running Fabric OS v5.3.0 or later with a maximum count of 5000 LSANs and the standby CP is running an earlier firmware version, then HA synchronization will fail. If 5000 is selected before downgrading to an earlier version of Fabric OS, you will be asked to go back to the default maximum LSAN count of 3000.
- Proxy Device Slots—The display shows the maximum versus the currently used proxy device slots. A proxy device is presented to an edge fabric as being connected to a translate domain slot. A slot is the port number and AL_PA combination. The slot-to-device WWN association is persistently stored. The physical and proxy devices use the 10000 device slots.
- Displays the maximum pool size for translate phantom node and port WWNs and shows the number of translate node and port WWNs from this pool.
- Phantom Node WWN—The display shows the maximum versus the currently allocated phantom switch node WWNs. The phantom switch requires node WWNs for FSPF and manageability purposes. Phantom node names are allocated from the pool sequentially and are not reused until the pool is exhausted and rolls over. The last allocated phantom node WWN is persistently stored. If the switch is disabled, the phantom node WWNs are not returned to the pool until the system reboots, because the phantom switch could still be accessible through other switches. Across a switch reboot, the allocation starts from the next usable WWN from the pool and not from the beginning.
- Phantom Port WWNs—The display shows the maximum versus the currently used phantom domain port WWNs. Phantom domain ports require port WWNs for manageability purposes. Phantom domain ports include ports connecting front and translate domains (virtual ISLs), translate domain ports for proxy devices, and EX_Ports. Phantom port names are allocated from the pool sequentially and are not resumed until the pool is exhausted and rolls over. The last allocated phantom port WWN is persistently stored. If the switch is disabled, phantom port WWNs are not returned to the pool until the system reboots, because the phantom switch may still be accessible through other switches. Across the switch reboot, the allocation starts from the next usable WWN base from the pool and not from the beginning.
- Max proxy devices—The maximum versus the currently used proxy devices.
- Max NR_Port—The maximum versus the currently used NR_Port entries. Destination NR_Port entries are stored at every physical port for routing decision purposes.
The following example shows the use of the `fcrResourceShow` command display per physical port (EX_Port) resources.

```
switch:admin> fcrresourceshow
Daemon Limits:
Max Allowed Currently Used
----------------------------------
LSAN Zones: 3000 28
LSAN Devices: 10000 51
Proxy Device Slots: 10000 20
WWN Pool Size Allocated
----------------------------------
Phantom Node WWN: 8192 5413
Phantom Port WWN: 32768 16121
Port Limits:
Max proxy devices: 2000
Max NR_Ports: 1000
Currently Used(column 1: proxy, column 2: NR_Ports):
0 | 0 34
1 | 3 34
4 | 0 0
5 | 0 0
6 | 0 0
7 | 0 0
8 | 6 34
9 | 6 34
10 | 6 34
11 | 6 34
12 | 6 34
13 | 6 34
14 | 6 34
15 | 6 34
16 | 8 34
17 | 8 34
18 | 8 34
19 | 8 34
20 | 8 34
21 | 8 34
22 | 8 34
23 | 8 34
```

See the Fabric OS Command Reference for details about the `fcrResourceShow` command.

**Routing ECHO**

The FC-FC Routing Service enables you to route the ECHO generated when an `fcPing` command is issued on a switch, providing `fcPing` capability between two devices in different fabrics across the 400 MP Router, or 4/256 SAN Director or DC Director with an FR4-18i blade.
To check for Fibre Channel connectivity problems:

1. **On the edge Fabric OS switch**, make sure that the source and destination devices are properly configured in the LSAN zone before entering the `fcPing` command. This command performs the following functions:
   - Checks the zoning configuration for the two ports specified.
   - Generates an ELS (extended link service) ECHO request to the source port specified and validates the response.
   - Generates an ELS ECHO request to the destination port specified and validates the response.

   ```
   switch:admin> fcping 0x060f00 0x05f001
   Source: 0x60f00
   Destination: 0x5f001
   Zone Check: Zoned
   ``

   Pinging 0x60f00 with 12 bytes of data:
   received reply from 0x60f00: 12 bytes time:501 usec
   received reply from 0x60f00: 12 bytes time:437 usec
   received reply from 0x60f00: 12 bytes time:506 usec
   received reply from 0x60f00: 12 bytes time:430 usec
   received reply from 0x60f00: 12 bytes time:462 usec
   5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
   Round-trip min/avg/max = 430/467/506 usec

   Pinging 0x5f001 with 12 bytes of data:
   received reply from 0x5f001: 12 bytes time:2803 usec
   received reply from 0x5f001: 12 bytes time:2701 usec
   received reply from 0x5f001: 12 bytes time:3193 usec
   received reply from 0x5f001: 12 bytes time:2738 usec
   received reply from 0x5f001: 12 bytes time:2746 usec
   5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
   Round-trip min/avg/max = 2701/2836/3193 usec

2. **Regardless of the device’s zoning configuration**, the `fcPing` command sends the ELS frame to the destination port. A destination device can take any one of the following actions:
   - Send an ELS Accept to the ELS request.
   - Send an ELS Reject to the ELS request.
   - Ignore the ELS request.

   There are some devices that do not support the ELS ECHO request. In these cases, the device will either not respond to the request or send an ELS reject. When a device does not respond to the ELS request, further debugging is required; however, do not assume that the device is not connected.

   For details about the `fcPing` command, see the Fabric OS Command Reference.

**Upgrade and downgrade considerations**

If you downgrade to a version of Fabric OS that does not support FC-FC Routing Services, then your FC-FC routing configuration will be lost. Brocade recommends that you enter the `configUpload` command to save your FC-FC routing configuration before performing any downgrades. For further instructions on downgrading, refer to “Installing and maintaining firmware” on page 23.

**Interoperability with legacy FCR switches**

The following interoperability considerations apply when administering legacy FCR switches in the same BB fabric as switches supporting Fabric OS v5.2.0 or later:

- When a legacy switch is connected to the backbone fabric, a RASLog message is issued indicating that the capability of the BB fabric is lower as legacy FCR switches (those with XPath OS and Fabric OS 5.1) support lower capability limits.
- If an XPath OS switch joins the BB fabric, a RASLog message is issued indicating that the backbone-to-edge fabric is not supported with the XPath OS switch.
For the exact RASLog message descriptions, see the following RASLogs: FCR_1055, FCR_1056, and FCR_1073. For further information on these messages, refer to Fabric OS Message Reference.

**Backward compatibility**

In a fabric with Secure Fabric OS enabled, the edge fabric must have Fabric OS 3.2, 4.4.0, or later because only DH-CHAP authentication is supported.

For a nonsecure fabric, the hardware and firmware compatibility is described in Table 57.

**Table 57**  Hardware and firmware compatibility for nonsecure fabrics

<table>
<thead>
<tr>
<th>Model</th>
<th>Supported version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2Gb SAN Switches</td>
<td>Fabric OS 2.6.1 or later</td>
</tr>
<tr>
<td>SAN Switch 2/8 EL, SAN Switch 2/16 EL, SAN Switch 2/16</td>
<td>Fabric OS 3.1.0 or later</td>
</tr>
<tr>
<td>SAN Switch 2/32, Core Switch 2/64</td>
<td>Fabric OS 4.1.0x or later</td>
</tr>
<tr>
<td>SAN Switch 2/8V, SAN Switch 2/16V, SAN Director 2/128</td>
<td>Fabric OS 4.2.0x or later</td>
</tr>
<tr>
<td>SAN Switch 4/32</td>
<td>Fabric OS 4.4.0 or later</td>
</tr>
<tr>
<td>4/8 SAN Switch, 4/16 SAN Switch, 4/256 SAN Director</td>
<td>Fabric OS 5.0.1 or later</td>
</tr>
<tr>
<td>4/64 SAN Switch, 400 MP Router</td>
<td>Fabric OS 5.1.0 or later</td>
</tr>
<tr>
<td>Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP c-Blade</td>
<td>Fabric OS 5.2.0 or later</td>
</tr>
<tr>
<td>4/256 SAN Director with FC4-16, FC4-48, or FC4-16IP blades</td>
<td>Fabric OS 5.2.0 or later</td>
</tr>
<tr>
<td>4/256 SAN Director with FC10-6</td>
<td>Fabric OS 5.3.0 or later</td>
</tr>
<tr>
<td>SAN Switch 4/32B</td>
<td>Fabric OS 5.3.0 or later</td>
</tr>
</tbody>
</table>

**Front domain consolidation**

The FCR switch is connected to the edge fabrics using EX_Ports or VEX_Ports. On prior FCR releases (XPath 7.1.2, 7.3, 7.4 and Fabric OS 5.1) every EX_Port connecting to an edge fabric projects its own front domain. For example, if there are three EX_Ports connected from the router to the edge fabric, there will be three front domains projected to the edge fabric.

The Front Domain Consolidation is when one front domain from a single FCR is projected to the edge fabric regardless of the number of EX_Ports connected from that router to the edge fabric. The front domain is consolidated only within the FCR switch. Another router connected to the same edge fabric projects a different front domain.

Front domain consolidation conserves resources on the FCR switch. Expanded use of FCR switches with multiple EX_Ports connected to the same edge fabric raises the overhead of projecting a front domain for each EX_Port and quickly uses up resources within the edge fabric and resource consumption on the FC router.

In releases prior to 5.2.0, every EX_Port connected to the same edge fabric had a unique domain and unique domains require separate WWNs. With front domain consolidation, the domain is the same for all ports connected to the same edge fabric from the FC router, so in this case the WWN will be the same.

**Using front domain consolidation**

To support the consolidated front domain feature, existing CLI and API commands are used to manage and configure the router. Existing CLI commands offer additional options to support the front domain consolidation feature.
The `portCfgExport` command has additional options to verify the front Domain ID. The `portCfgExport -d` option is changed to enforce use of the same front Domain ID for the EX_Ports connected to the same edge fabric. The `portCfgExport` display results remain the same.

For more information about the `portCfgExport -d` option, see “portCfgExport options” on page 226 and the command details in the Fabric OS Command Reference.

The following example illustrates the use of the `portcfgexport` command.

```
switch:admin_06> portcfgexport 2/0
Port 2/0 info
Admin: enabled
State: OK
Pid format: core(N)
Operate mode: Brocade Native
Edge Fabric ID: 16
Front Domain ID: 160
Front WWN: 50:06:06:9e:20:9f:ce:10
Principal Switch: 7
principal WWN: 10:00:00:60:69:c0:05:8a
Fabric Parameters: Auto Negotiate
R_A_TOV: 9000(N)
E_D_TOV: 2000(N)
Edge fabric's primary wwn: N/A
Edge fabric's version stamp: N/A
```

The `fabricShow` command shows only one front domain per router connection. In the following example displayed below is from an edge fabric and shows that `fcr_fd_3_32` has two EX_Ports connections, but one front Domain ID.

```
switch:admin_06> fabricshow
Switch ID Worldwide Name Enet IP Addr FC IP Addr Name
-------------------------------------------------------------------------
1: fffc01 50:00:51:e3:70:d2:5f:cb 0.0.0.0 0.0.0.0 "fcr_xd_1_32"
2: fffc02 50:00:51:e3:70:d2:5f:cc 0.0.0.0 0.0.0.0 "fcr_xd_2_1"
3: fffc03 50:00:51:e3:60:14:0e:20 0.0.0.0 0.0.0.0 "fcr_fd_3_32"
199: fffcc7 10:00:00:60:69:c0:05:d1 10.32.156.33 0.0.0.0 "mojo__10"
"mojo__10" The Fabric has 4 switches
```

For more information about the `fabricShow` command, see the Fabric OS Command Reference.

**Range of output ports**

The edge fabric detects only one front domain from an FC router connected through multiple output ports. The output port of the front domain is not fixed to 0; the values can be in a range of 129–255. The range of the output ports connected to the xlate domain is also 129–255. This range enables the front domain to connect to 127 remote xlate domains.
To display the range of output ports connected to the xlate domains:

1. Log in to the FC router.
2. Enter the `lsDbShow` command on the edge fabric.

   The following example shows the range of output ports.

   ```
   linkCnt = 2, flags = 0x0
  LinkId = 53, out port = 1, rem port = 35, cost = 500, costCnt = 0, type = 1
  LinkId = 57, out port = 129, rem port = 18, cost = 500, costCnt = 0, type = 1
   ```

   The following example also shows the use of the `lsDbShow` display on the edge fabric. The front domain, domain 3, has two links representing two EX_Port connections with output ports 129 and 132.
   Domain = 3, Link State Database Entry pointer = 0x100bbcc0
   ```
   linkCnt = 4, flags = 0x0
  LinkId = 199, out port = 129, rem port = 2, cost = 10000, costCnt = 0, type = 1
  LinkId = 199, out port = 132, rem port = 3, cost = 10000, costCnt = 0, type = 1
  LinkId = 2, out port = 1, rem port = 2, cost = 10000, costCnt = 0, type = 1
  LinkId = 1, out port = 32, rem port = 2, cost = 10000, costCnt = 0, type = 1
   ```

To verify normal operation:

1. Connect the FC router to an edge fabric switch through multiple EX_Ports from the same router.
2. Confirm that the ports are enabled with `portCfgShow`.
3. Confirm that the EX_Ports share the same front Domain ID (DID) and node WWN, using the `portCfgExport` command.

**NOTE:** Abnormal operation for front domain consolidation exists when the ports do not come online or in the Normal Operation setup described previously. The EX_Ports do not share the same front domain consolidation PID and node WWN.

In case of an unexpected failure, run and save the output from the commands `supportShow`, or `supportSave` if not supported, on each of the FC routers and edge switches.
Interoperating with an M-EOS fabric

**IMPORTANT:** Interoperating with an M-EOS fabric is not supported at the time of the release of this document. Please check with your sales representative or [http://www.hp.com](http://www.hp.com) regarding HP support of the interoperability features.

This section covers how to set up your B-Series SAN and M-Series SAN to route traffic without merging the two SANs. If you want to merge the SANs or use SANtegrity, refer to “Implementing an interoperable fabric” on page 481 for more information.

The FC router interoperates with M-EOS fabrics in both the McDATA Open Mode 1 and the McDATA Fabric Mode. Fabric OS 6.0 provides the ability to configure any EX_Port to connect to a M-EOS fabric by using an E_Port without disrupting the existing services. All the EX_Port functionality, such as fabric isolation and device sharing, remains the same as connecting to an existing Brocade fabric.

**NOTE:** M-EOS fabrics will be supported only as edge fabrics and should not be connected directly into the backbone.

Fabric OS 6.0 interoperates with M-EOS edge fabrics in Fabric Mode and Open Mode 1 and will support the LSAN zone with the backbone devices. Table 58 on page 249 outlines which releases of Fabric OS are compatible with which releases of M-EOS.

**Table 58** Brocade-McDATA M-EOSc interoperability compatibility matrix

<table>
<thead>
<tr>
<th>Fabric OS</th>
<th>Versions of M-EOSc</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.0</td>
<td>Yes</td>
</tr>
<tr>
<td>5.2.0</td>
<td>No</td>
</tr>
<tr>
<td>5.3.0</td>
<td>No</td>
</tr>
<tr>
<td>6.0</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Both Open and McDATA Fabric modes are supported.
2. Fabric OS 5.1.0 and M-EOSc 4.1.1, 5.1.2, 6.2.0 can interoperate through the FC routing capability of the MP Router only. Fabric OS and M-EOSc 7.1.3 can interoperate through the FC routing capability of the MP Router, 400 MP Router, or FR4-18i blade. Fabric OS and M-EOSc 8.0.0 and 9.2.0 can interoperate through the FC routing capability of the 400 MP Router, or FR4-18i blade.
The Fibre Channel routing feature for M-EOS interoperability is not a licensed feature.

Table 59  Brocade-McDATA M-EOS interoperability compatibility matrix

<table>
<thead>
<tr>
<th>Fabric OS</th>
<th>Versions of M-EOSn (i10k)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9.2.0</td>
</tr>
<tr>
<td>v5.3.0</td>
<td>Yes</td>
</tr>
<tr>
<td>6.0</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Both Open and McDATA Fabric modes are supported.

Connected SANs provide additional functionality not possible with segregated SANs. Some of these functions are as follows:

- Island consolidation—Uses the Fabric OS 6.0 FC router to connect isolated M-EOS and Brocade Fabrics and share devices.
- Backup consolidation—Consolidates backup solutions across Brocade and M-EOS fabrics.
- Manageable large-scale storage network—Uses the Fabric OS 6.0 FC router to localize traffic while connecting devices in the metaSAN. This provides a large number of fabrics with a large number of devices.
- Sharing across an FCIP link—Shares devices between Brocade and M-EOS fabrics over a campus Ethernet or over long-distance IP links beyond 1000 km.
- Sharing across a long-distance FC link—Shares devices between Brocade fabrics over long-distance FC links as far as 300 km.
- LUN sharing—Uses your high-end RAID array connected to an Intrepid series to share targets with an HP fabric; just connect one Intrepid series port to an FC router EX_Port and the one EX_Port to the HP fabric.
- LSAN zone database binding—Increases FCR scalability to support more FCR switches in the backbone and support more devices in the metaSAN.

The connectivity limitations of a metaSAN containing Brocade and M-EOS fabrics are defined by the scalability of each individual fabric. See the HP StorageWorks SAN Design reference guide for the latest scalability support information:

http://www.hp.com/go/sandesignguide

Refer to the M-EOS fabric documentation for scalability considerations.

McDATA Mi10K interoperability

When an EX_Port is connected to a M-EOS edge fabric, the front Domain ID must be within a range the edge M-Series switch can understand. Valid values are:

- McDATA Native mode: 1 - 31
- McDATA Open mode: 97 - 127

The default front Domain ID assigned to the EX_Port remains at 160 when it is created. However when connected to the Mi10K, a daemon sends a request Domain ID (RDI) command that must be within the valid range M-EOS understands.

When an RDI command is sent to an Mi10K switch with a valid Domain ID defined by standards and is not within the range an Mi10K switch understands, the RDI request is rejected. This behavior of the i10k is different from other M-Series switches.

If you set a front Domain ID that is not within the valid range M-EOS understands, then in Fibre Channel routing, a daemon internally requests a valid Domain ID that M-EOS understands. Unless you change the front Domain ID, there is no impact.

The behavior with the non-Mi10k switches displays the regular switch when configured. When the Mi10k is connected, it shows the switch name in format "McDATA:<IpAddr> format".

First the daemon requests the switch name and when this request is rejected by the Mi10K edge switch with the reason of command not supported, the daemon will try an ELS command request node identification.
data (RNID) to obtain the information. If the command to get the switch name is successful, the RNID request is not tried and the switch name is obtained. See the following example:

```
switch: admin> switchshow | grep EX
44  3   12   042c00   id    N2   Online     EX-Port
 10:00:08:00:88:2c:c2:00  "McDATA:10.32.68.146" (fabric id = 12 )
46  3   14   042e00   id    N2   Online     EX-Port
 10:00:00:60:69:e2:18:b6  "b24000_5x_1" (fabric id = 23 ) (Trunk master)
```

```
switch: admin> fcrfabricshow
FC router WWN: 10:00:00:60:69:80:04:0a, Dom ID:   4, Info: 10.32.66.25, "b12000_5x_1"
EX_Port       FID    Neighbor Switch Info (WWN, enet IP, name)
------------------------------------------------------------------------
44         12     10:00:08:00:88:2c:c2:00   10.32.68.146  "McDATA:10.32.68.146"
46         23     10:00:00:60:69:e2:18:b6   10.32.66.12      "b24000_5x_1"
```

To enable the interoperability a new parameter `-m` has been added to the command `portcfgexport`.

```
portcfgexport <port_number> -m <0|1|2|3>
```

Where `<port_number>` is the port number, 0 is for Brocade Native mode; this is the default parameter. ‘1’ is for McDATA Open Mode 1. ‘2’ is for McDATA Fabric Mode, it is used when the neighboring M-Series switch is running OS version such as 8.2.0 or later. The `-m 3` option is used for legacy M-EOS versions such as 5.0.2.

When the command is issued with the port number as the only parameter, the current operational mode of the EX_Port is displayed.

The following command sequence is an example to connect port 5 to a McDATA fabric in McDATA native Mode:

```
switch:admin> portdisable 5
switch:admin> portcfgexport 5 -m 2
switch:admin> portenable 5
```

Once the port is properly configured and connected, doing `switchShow` on the FCR it will show the M-Series switch that’s connected. From the M-EOS side, the `show` command will also show the front domain. If the LSAN is configured and the proxy devices are created, the proxy device will show up in the name server of the edge fabric. Also the xlate domain will show in the fabric of the edge fabric.

**Configuring the fabrics for interconnectivity**

When connecting a Brocade fabric with a M-EOS fabric using an FC router, you must configure the switch on both fabrics as well as the router, as described in the following sections:

- “Connectivity modes” on page 251
- “Configuring the FC router” on page 251
- “Configuring M-EOS for interconnection” on page 254
- “Completing the configuration” on page 258

**NOTE:** Trunking is not supported on EX_Ports connected to the M-EOS fabric.
You can connect to M-EOS fabrics in both McDATA Open mode or McDATA Fabric mode. If the mode is not configured correctly, the port is disabled because of incompatibility.

To allow interconnectivity with M-EOS SANs, the command line interface (CLI) command `portCfgExPort` uses the `-m` option to indicate the connectivity mode. Table 60 lists the valid parameters to use with the `-m` option to set the connectivity mode.

**Table 60  portCfgExPort -m values**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Brocade Native</td>
<td>Default mode.</td>
</tr>
<tr>
<td>1</td>
<td>McDATA Open Mode 1</td>
<td>When the neighboring McDATA switch is running in open mode.</td>
</tr>
<tr>
<td>2</td>
<td>McDATA Fabric Mode (native mode)</td>
<td>When the neighboring McDATA switch is running in native mode.</td>
</tr>
<tr>
<td>3</td>
<td>McData Fabric legacy mode</td>
<td>Not currently used.</td>
</tr>
</tbody>
</table>

You can display the current operational mode of the EX_Port by issuing the `portCfgExPort` command with the port number as the only parameter.

See “Configuring an interfabric link” on page 225 for details about the `portCfgExPort` command, which is used for McDATA Fabric mode on Fabric OS v5.2.0 or later.

**Configuring the FC router**

When configuring an HP fabric to connect to a Native McDATA fabric, you must perform some preparation on the FC router. The following procedure shows how to connect an EX_Port of an FC router fabric to a Native McDATA fabric configured in Fabric mode.

1. Verify the Native McDATA firmware version. To display the front domain on the M-EOS fabric, use the M-EOS `show` command.
2. Using the `version` command, make sure that Fabric OS 6.0 is installed on the 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade, as shown in the following example:

```bash
fcr_switch:AD255:admin> version
Kernel:     2.4.19
Fabric OS:  v6.0
Made on: Thu Sep 21 01:15:34 2006
Flash:      Fri Sep 22 20:53:48 2006
BootProm:   4.5.3
```
3. On the 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade, use the
\texttt{portDisable} to disable the EX\_Port that you will use to connect to the M-Series switch. Ports are
persistently disabled by default.

\begin{verbatim}
Switch:admin_06> portdisable 10/13
\end{verbatim}

```
Switch:admin_06> switchshow
```
```
switchName: b48000_5x_1/PORT/P
switchType: 42.2
switchState: Online
switchMode: Native
switchRole: Principal
switchDomain: 3
switchId: fffc03
switchWwn: 10:00:00:60:69:e4:00:86
zoning: ON (test)
switchBeacon: OFF
blade3 Beacon: OFF
blade8 Beacon: OFF
blade10 Beacon: OFF
FC router: ON
FC router BB Fabric ID: 1

Index Slot Port Address Media Speed State  Proto
-----------------------------------------
112 10 0 037000 id N4 No\_Light         Disabled (Persistent)
113 10 1 037100 id N4 No\_Light         Disabled (Persistent)
114 10 2 037200 id N4 No\_Light         Disabled (Persistent)
115 10 3 037300 id N4 No\_Light         Disabled (Persistent)
116 10 4 037400 id N4 No\_Light         Disabled (Persistent)
117 10 5 037500 id N4 No\_Light         Disabled (Persistent)
118 10 6 037600 id N4 No\_Light         Disabled (Persistent)
119 10 7 037700 id N4 No\_Light         Disabled (Persistent)
120 10 8 037800 id N4 No\_Sync          Disabled (Persistent)
121 10 9 037900 id N2 No\_Light         Disabled (Persistent)
122 10 10 037a00 id N2 No\_Light         Disabled (Persistent)
123 10 11 037b00 id N2 No\_Light         Disabled (Persistent)
124 10 12 037c00 id N2 Online          EX-Port
10:00:00:05:1e:34:e0:6a "b4100_5x_1"(fabric id = 41 )
125 10 13 037d00 id N2 In\_Sync          Disabled (Persistent)
126 10 14 037e00 id N2 No\_Light         Disabled (Persistent)
127 10 15 037f00 id N2 No\_Light         Disabled (Persistent)
240 10 16 03f000 -- -- Offline           Disabled (Persistent)
241 10 17 03f100 -- -- Offline           Disabled (Persistent)
242 10 18 03f200 -- -- Offline           Disabled (Persistent)
243 10 19 03f300 -- -- Offline           Disabled (Persistent)

...this example has been truncated
```

4. Issue the \texttt{portCfgExPort} command to configure the port as an EX\_Port with a different FID within
the McDATA Fabric Mode.

This port can now connect to a M-Series switch in a McDATA Fabric mode or McDATA Open mode.
The following example sets port 10/13 to admin-enabled, assigns a Fabric ID of 37, and sets the
M\_EOS connection to McDATA Fabric Mode.

```
switch:admin_06> portcfgexport 10/13 -a 1 -f 37 -m 2
```
5. Enable the port by issuing the `portEnable` command.

```
switch>:admin_06> portenable 10/13
```

If the port was persistently disabled, use the following command to enable the port:

```
switch>:admin_06> portcfgpersistentenable 10/13
```

- Connect IFL1 and verify EX_PORT connectivity. Repeat for all Brocade fabric IFLs.
- Connect IFL (n) for the M-EOS fabric and verify EX_PORT connectivity. Repeat for all M-EOS fabric IFLs.

6. Log in to the FC router and issue the `switchShow` command to display the M-Series switch that is connected to the FC router EX_Port. The following example illustrates the use of the `switchShow` command and its output.

```
switch>:admin_06> switchshow
switchName: b48000_5x_1
switchType: 42.2
switchState: Online
switchMode: Native
switchRole: Principal
switchDomain: 3
switchId: fffc03
switchWwn: 10:00:00:60:69:e4:00:86
zoning: ON (test)
switchBeacon: OFF
blade3 Beacon: OFF
blade8 Beacon: OFF
blade10 Beacon: OFF
FC router: ON
FC router BB Fabric ID: 1
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Slot</th>
<th>Port</th>
<th>Address</th>
<th>Media</th>
<th>Speed</th>
<th>State</th>
<th>Proto</th>
</tr>
</thead>
<tbody>
<tr>
<td>112</td>
<td>10</td>
<td>0</td>
<td>037000</td>
<td>id</td>
<td>N4</td>
<td>No_Light</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>113</td>
<td>10</td>
<td>1</td>
<td>037100</td>
<td>id</td>
<td>N4</td>
<td>No_Light</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>114</td>
<td>10</td>
<td>2</td>
<td>037200</td>
<td>id</td>
<td>N4</td>
<td>No_Light</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>115</td>
<td>10</td>
<td>3</td>
<td>037300</td>
<td>id</td>
<td>N4</td>
<td>No_Light</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>116</td>
<td>10</td>
<td>4</td>
<td>037400</td>
<td>id</td>
<td>N4</td>
<td>No_Light</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>117</td>
<td>10</td>
<td>5</td>
<td>037500</td>
<td>id</td>
<td>N4</td>
<td>No_Light</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>118</td>
<td>10</td>
<td>6</td>
<td>037600</td>
<td>id</td>
<td>N4</td>
<td>No_Light</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>119</td>
<td>10</td>
<td>7</td>
<td>037700</td>
<td>id</td>
<td>N4</td>
<td>No_Light</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>120</td>
<td>10</td>
<td>8</td>
<td>037800</td>
<td>id</td>
<td>N4</td>
<td>No_Sync</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>121</td>
<td>10</td>
<td>9</td>
<td>037900</td>
<td>id</td>
<td>N2</td>
<td>No_Light</td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>10</td>
<td>10</td>
<td>037a00</td>
<td>id</td>
<td>N2</td>
<td>No_Light</td>
<td></td>
</tr>
<tr>
<td>123</td>
<td>10</td>
<td>11</td>
<td>037b00</td>
<td>id</td>
<td>N2</td>
<td>No_Light</td>
<td></td>
</tr>
<tr>
<td>124</td>
<td>10</td>
<td>12</td>
<td>037c00</td>
<td>id</td>
<td>N2</td>
<td>Online</td>
<td>EX-Port</td>
</tr>
<tr>
<td>125</td>
<td>10</td>
<td>13</td>
<td>037d00</td>
<td>id</td>
<td>N2</td>
<td>Online</td>
<td>EX-Port</td>
</tr>
<tr>
<td>126</td>
<td>10</td>
<td>14</td>
<td>037e00</td>
<td>id</td>
<td>N2</td>
<td>No_Light</td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>10</td>
<td>15</td>
<td>037f00</td>
<td>id</td>
<td>N2</td>
<td>No_Light</td>
<td></td>
</tr>
<tr>
<td>240</td>
<td>10</td>
<td>16</td>
<td>03f000</td>
<td>--</td>
<td>--</td>
<td>Offline</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>241</td>
<td>10</td>
<td>17</td>
<td>03f100</td>
<td>--</td>
<td>--</td>
<td>Offline</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>242</td>
<td>10</td>
<td>18</td>
<td>03f200</td>
<td>--</td>
<td>--</td>
<td>Offline</td>
<td>Disabled (Persistent)</td>
</tr>
<tr>
<td>243</td>
<td>10</td>
<td>19</td>
<td>03f300</td>
<td>--</td>
<td>--</td>
<td>Offline</td>
<td>Disabled (Persistent)</td>
</tr>
</tbody>
</table>

...this example has been truncated

7. You can now physically attach your ISLs from the 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade to the switches.

ISLs apply only to Brocade switches that are not connected as an edge fabric (IFLs). When an M-Series switch is present, it is assumed that you are creating an edge fabric.
For information about Brocade edge fabric setup on E_Ports and interswitch linking, see “Administering ISL Trunking” on page 129. For information on EX_Port Frame trunking setup on the FCR switch, see “Using EX_Port frame trunking” on page 234.

8. Capture a SAN profile of the McDATA and Brocade SANs, identifying the number of devices in each SAN.

By projecting the total number of devices and switches expected in each fabric when the LSANs are active, you can quickly determine the status of the SAN by issuing the commands `nsAllShow` and `fabricShow` on the Brocade fabric. The `nsAllShow` displays the global name server information and `fabricShow` displays the fabric membership information. The following examples illustrate the use of these commands.

The switch symbolic name. An arrow (>) indicates the principal switch.

```
switch:admin> fabricshow

Switch ID Worldwide Name Enet IP Addr FC IP Addr Name
-------------------------------------------------------------------------
64: fffe40 10:00:00:60:69:00:06:56 192.168.64.59 192.168.65.59 "sw5"
65: fffe41 10:00:00:60:69:00:02:0b 192.168.64.180 192.168.65.180 >"sw180"
66: fffe42 10:00:00:60:69:00:05:91 192.168.64.60 192.168.65.60 "sw60"
67: fffe43 10:00:00:60:69:10:60:1f 192.168.64.187 0.0.0.0 "sw187"
```

The Fabric has 4 switches.

You can use SAN Pilot or EFCM to gather similar information for the M-EOS fabric.

![EFCM SAN status](image)

When you have configured the 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade to connect to a Brocade fabric, you must create LSAN zones for the SAN. Once you have set up LSAN zoning, you can issue the `cfgShow` command to verify that the zoning is correct.

**Configuring M-EOS for interconnection**

To ensure connectivity with the fabric, you must prepare the M-EOS fabric for use with the 400 MP Router and 4/256 SAN Director or DC Director with an FR4-18i blade.

---

### NOTE:  
The procedures described in this section were current when the document was written, but may have changed since then. Refer to the Zoning User Manual available per the HP switch web page.

---

To prepare the M-EOS fabric:

**1.** Log in to SAN Pilot or basic EFC Manager depending upon the firmware release.

**2.** From the SAN Pilot left navigation menu, select **Configure**.

**3.** Select the **Zoning** tab, then select the **Zones** tab. (select **Configure > Zoning** on EFCM).

The FCR can support up to 2048 zones when connected to an M-Series 9.6 switch.
4. Type the desired name in the Zone Name field, using the LSAN_xxxx naming schema.
   In EFCM, move to the Zone Name field, and enter the desired name using the LSAN_xxxx naming schema.
5. In SAN Pilot, click the **Add button to add the specified zone.**
   As shown in the following illustration, when you add the new zone name, the name is displayed in the Pending Zone Set list.
6. To add devices that are connected to the Brocade fabric, click **Edit** in the **Pending Zone** set.

7. On the **Modify Zone** tab, enter the device WWN into the World Wide Name field and click **Add**. The **Pending Zone Membership List** is updated with the new Zone members.
   If you are using EFCM, select **Potential Zone Members > New Member**, enter the WWN port name, and click **Add**.

**NOTE:** The procedures described in this section were current when the document was written, but may have changed since then. Refer to the **Zoning User Manual** available per the HP switch product web page.

8. Select the **Zone Set** tab in SAN Pilot.
   If you are using EFCM or the **Zoneset** Library window, tab to **Zone Sets** and select **File > New**.

9. Enter a name for the Pending Zone set in **Zone Set Name** and select **Rename**.
   The steps for EFCM will be similar.

10. Click **Save** and **Activate the Pending Zone** set.
    The zones in the Pending Zone set are added to the Zone Set that you specified.
    In EFCM, return to the main window and select **Configure**, then select **Activate Zone Set** to launch the zone set activation window. Highlight the zone set to be activated and click **Next**. Click **Next** again, then **Start** to activate the zone set.
Regardless of the method used, you should now verify that the new zone set containing your LSAN has been added.

Alternately, use the following procedure:

1. Create the LSAN, using the LSAN_xxxx naming schema.
2. Append the newly-created zone set to a currently active zone set.
3. Activate the updated zone set.

**LSAN zoning with M-EOS**

An LSAN is defined by a zone in an edge fabric. When zoning an LSAN containing multiple manufacturers’ fabrics (such as a Brocade-Cisco SAN), you must use port WWN. Because port IDs are not necessarily unique across fabrics, you cannot use the `domain,port` method of identification.

If the LSAN is configured and the proxy devices are created, the proxy device will show in the name server of the edge fabric and the xlate domain will show in the fabric of the edge fabric.

For more details about LSAN zoning, see “Configuring LSANs and zoning” on page 235.

If the LSAN devices appear in only one of the fabrics in a multiple-fabric SAN, use the following procedure to correct the problem.

To correct errors if LSAN devices appear in only one of the fabrics:

1. Log in to each fabric and verify that all of the devices are physically logged in.
2. Verify that the devices are properly configured in the LSAN zone in both edge fabrics.
4. Use M-EOS EFCM or SAN Pilot to verify the M-EOS fabric, including the front and translation domains.
5. Move back to the 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade and issue the `fcrProxyDevShow` command on to verify that the devices are configured and exported.

```
switch:admin> fcrproxydevshow
```

<table>
<thead>
<tr>
<th>Proxy</th>
<th>WWN</th>
<th>Proxy PID</th>
<th>Device Exists</th>
<th>Physical PID</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>20:00:00:01:73:00:59:dd</td>
<td>05f001</td>
<td>12</td>
<td>610902</td>
<td>Imported</td>
</tr>
<tr>
<td>10</td>
<td>21:00:00:e0:8b:04:80:76</td>
<td>02f002</td>
<td>11</td>
<td>340713</td>
<td>Imported</td>
</tr>
<tr>
<td>10</td>
<td>50:06:01:68:40:04:d3:95</td>
<td>02f001</td>
<td>11</td>
<td>660713</td>
<td>Imported</td>
</tr>
<tr>
<td>11</td>
<td>10:00:00:00:c9:2d:3d:5c</td>
<td>020001</td>
<td>10</td>
<td>011500</td>
<td>Imported</td>
</tr>
<tr>
<td>11</td>
<td>50:06:01:60:40:04:d3:95</td>
<td>020002</td>
<td>10</td>
<td>011400</td>
<td>Imported</td>
</tr>
</tbody>
</table>

6. Connect to the switch and configure the connection to capture console output.

7. Issue the `supportShow` (or `supportSave` if available) command, and save the output.

8. If the fabric does not appear:
   a. Disable the EX_Port on the connected fabric.
   b. Issue the `portLogClear` command for the port.
   c. Enable the port on the 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade.
   d. Issue the `portLogDump` command for the port, capturing the output.

Use the `portLogDump` tool to troubleshoot the problem, using the command output.

If an EX_Port connecting a 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade and an edge fabric is disabled due to an error, the error causing that port’s most recent disabled state appears in the `switchShow` command output. This error appears until that port comes back online, even after the cables have been detached from the port.

To remove the error listing in the `switchShow` output, reboot the 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade. An example of the type of error displayed is ‘Incompatible port mode’.

Completing the configuration

After you prepare the M-Series switch and the 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade for use, complete the configuration using the following procedure.

1. Physically connect the EX_Port that you configured for the Brocade switch to the FC router.
2. Log in to the Brocade switch as an admin.
3. Physically connect the configured FC router EX_Port to the M-Series switch, and issue the `switchShow` command on the Brocade FCR.

   New domains should be visible for each IFL (front domain) that connects the Brocade to the FC router and one domain for the translate domain.

4. Start SAN Pilot (or EFCM) and select the fabric for the M-Series switch.
5. View the fabric topology.

   New domains should be visible for every FCR connection to the M-Series switch to the 400 MP Router or 4/256 SAN Director or DC Director with an FR4-18i blade, and one domain for the translate domain.

In EFCM, the M-Series switch should appear green, and the front domains (as well as the translate domain) are grayed out and inaccessible: EFCM cannot manage them. Tab to `Zone` and verify that the zone set configuration is correct: a blue icon beside each entry indicates that the devices are logged in to the fabric.
6. Log in to the Brocade edge fabric switch and issue the `nsAllShow` or the `nsCamShow` command.

```
edgeswitch:admin> nsallshow
{010e00 020000 03f001 04f002
4 Nx_Ports in the Fabric }
```

```
edgeswitch:admin> nscamshow
nsCam show for remote switches:
Switch entry for 1
  state  rev    owner
  known  v520  0xfffc02
Device list: count 1
  Type Pid  COS  PortName                NodeName
  N 010e00; 3;10:00:00:00:01:00:00;10:00:00:00:00:00:01:00;
    Fabric Port Name: 20:0e:00:60:69:e2:18:b6
    Permanent Port Name: 10:00:00:00:01:00:01:00
    Port Index: 14
    Share Area: No
    Device Shared in Other AD: No

Switch entry for 3
  state  rev    owner
  known  410  0xfffc02
Device list: count 1
  Type Pid  COS  PortName                NodeName
  N 03f001; 2,3;10:00:00:00:c9:44:54:04;20:00:00:00:c9:44:54:04;
    FC4s: FCP
    NodeSymb: [36] "Emulex LP9002 FV3.92A2 DV5-5.10A10 "
    Fabric Port Name: 50:00:51:e3:70:9a:3d:e8
    Permanent Port Name: 10:00:00:00:c9:44:54:04
    Port Index: na
    Share Area: No
    Device Shared in Other AD: No

Switch entry for 4
  state  rev    owner
  known  v410  0xfffc02
Device list: count 1
  Type Pid  COS  PortName                NodeName
  N 04f002; 3;10:00:00:00:03:00:00;10:00:00:00:00:03:00:00;
    Fabric Port Name: 50:06:06:91:23:45:6a:13
    Permanent Port Name: 10:00:00:00:00:03:00:00
    Port Index: na
    Share Area: No
    Device Shared in Other AD: No
```
All of the devices from both LSANs should appear in the output. If the devices do not appear in the output, issue the `cfgShow` command to verify your zone configuration. Use the `cfgactvshow` command to display the zone configuration currently in effect. The following example illustrates the use of `cfgactvshow`.

```
switch:admin> cfgactvshow
Effective configuration:
  cfg:test
    zone:lsan_san
      10:00:00:00:00:03:00:00
      10:00:00:00:00:01:00:00
    zone:lsan_test
      50:06:01:60:38:e0:0b:a4
      10:00:00:00:c9:44:54:04
```

7. Log into the FC router and run the `lsanZoneShow` command to verify FIDs and devices to be shared among LSANs.

### Migrating from an MP Router to a 400 MP Router

This section describes how to upgrade routers in your fabric with the least disruption, while providing better performance and scalability. Improper implementation could lead to a change in the xlate Domain IDs and proxy device PIDs, which may cause disruption in the fabric.

#### Configurations

FC routers are deployed in different configurations in a fabric. Those configurations are listed in the following pages and steps have been provided to integrate the 400 MP Router in a fabric with the HP StorageWorks Multi-protocol Router. The figures in the following pages demonstrate how the 400 MP Router should be integrated into a specified configuration, whether it is non-redundant, redundant, or in a dual backbone configuration.

#### Non-redundant configuration

A 400 MP Router can be inserted into an existing metaSAN so that the old and new configuration form one redundant configuration. Before implementing this design, configure the new router’s EX_Ports and fabric IDs with the same configuration parameters. The new configuration will look like Figure 15 on page 260.

Figure 15 shows an example of a simple non-redundant configuration.

![Figure 15](image_url) Non-redundant router configuration

Follow the steps in “To configure the new router:” on page 262 to change the configuration parameters to be the same as on the old router, before it is introduced in the metaSAN.
Using the FC-FC routing service

Figure 16  Configuration during the upgrade

The switch Domain ID and BB fabric ID of the new FC router can be identical. Once the metaSAN is stable, EX_Ports on the new router are ‘active’, the old router can be taken out of the setup.

Redundant configuration

The configuration shown in Figure 17 on page 261, shows that old routers can be removed one by one. For example, FC router 2 can be replaced with the new FC router. You are expected to maintain the connections to the edge fabrics and the other router, same as with old router. Configuration parameters described in “To configure the new router:” on page 262 should also be preconfigured on the new routers and match with the routers being replaced. The same procedure can be repeated for FC router 1.

NOTE: During the swap, traffic flowing through the ISL is affected.

Figure 17 shows an example of a simple redundant configuration.

Dual backbone configuration

In the configuration shown in Figure 18, follow the steps described in “To configure the new router:” on page 262 for each FC router.

Following is the example of a dual backbone configuration.
Devices directly connected to router

In the Multi-protocol Router, end devices are allowed to be directly connected, but these devices cannot be imported to other edge fabrics (using LSAN zones). During the upgrade process, these devices will face disruption unless there is redundancy support provided from the device end. 400 MP Router allows the end devices to be imported to edge fabrics.

To configure the new router:

1. Log in to the new router as admin.
2. Enable FCR functionality on the 400 MP Router.
   - On Fabric OS v5.2.x and earlier use the `fcrenable` command.
   - On Fabric OS v5.3.0 and later use the `fosconfig –enable fcr` command.
3. Set respective fabric IDs while configuring each of the EX_Ports using the `portcfgexport -f` command.
4. Verify that the operating mode is native while configuring the EX_Port using the `portcfgexport -m` command.
5. Set the BB Fabric ID using the `fcrconfigure` command.
6. Set other fabric parameters using the `configure` command, if they are not default.
7. You may choose to manually configure the xlate Domain IDs on the new router, to match with old router using the `fcrxlateconfig` command.
8. You may choose to manually configure the Area and AL_PA portions of the proxy device PID, using the `fcrproxyconfig` command.
Using the FC-FC routing service
11 Administering FICON fabrics

This chapter provides procedures for managing FICON fabrics.

Overview of Fabric OS support for FICON

IBM Fibre Connection (FICON®) is an industry-standard, high-speed input/output (I/O) interface for mainframe connections to storage devices. Fabric OS supports intermix mode operations, in which FICON and Fibre Channel technology work together. For specific information about intermix mode and other aspects of FICON, refer to the IBM Redbook, FICON® Implementation Guide (SG24-6497-01), and IBM System Storage: Implementing an IBM SAN (SG24-6116-06).

The following Fabric OS standard features support FICON fabrics:

- **Port swapping**
  Redirects resources from a failed port to a healthy port without changing the FICON host configuration. Port swapping is available for both FICON and open system environments. Port swapping resolves situations in which the hardware has failed and the channel configurations cannot be changed quickly. Port swapping has minimal or no impact on other switch features.

- **Insistent Domain ID (IDID)**
  Allows the switch to insist on a specific Domain ID before joining a fabric. This feature guarantees that a switch operates only with its preassigned Domain ID.

- **The FICON MIB module**
  Addresses link incident data for FICON hosts and devices connected to a switch. It supplements other MIBs used to manage switches and should be used in conjunction with those other MIBs. For more information, see the Fabric OS MIB Reference.

- **Link incident detection, registration, and reporting**
  Provides administrative and diagnostic information.

- **Switch Connection Control (SCC) policy**
  Includes switch binding security methods that prevent unauthorized devices from joining a fabric.

These management tools provide further support:

- **Fabric Manager**
  Fabric Manager is an optional software program that can be used to manage a fabric that supports FICON and FCP devices and traffic. This is the recommended GUI management tool for FICON environments.

- **Web Tools**
  Web Tools is an embedded GUI management tool that can be used to manage a director (switch) that supports FICON and Fibre Channel Protocol (FCP) devices and traffic. Some licenses are installed and activated on the switch at the factory. Use a management interface to verify that the required licenses are installed and activated on the switch.

The Secure Access Control List (ACL) feature provides the following fabric, switch, and port binding features:

- **Fabric binding** is a security method for restricting switches within a multiple-switch fabric. The SCC policy prevents unauthorized switches from joining a fabric.

- **Switch binding** is a security method for restricting devices that connect to a particular switch. If the device is another switch, this is handled by the SCC policy. If the device is a host or storage device, the Device Connection Control (DCC) policy binds those devices to a particular switch. Policies range from completely restrictive to reasonably flexible, based upon customer needs.

- **Port binding** is a security method for restricting host or storage devices that connect to particular switch ports. The DCC policy also binds device ports to switch ports. Policies range from completely restrictive to reasonably flexible, based on customer needs.

SCC ACL with strict fabric-wide consistency is necessary for FICON switch binding.
Supported switches

FICON protocol is supported on the following HP StorageWorks models: DC SAN Backbone Director, short name, DC Director (FC8-16, FC8-32 port blades, FR4-18i FCIP blade and FC10-6 10 Gbit/sec port blade for ISL connections), the 4/256 SAN Director (FC4-16, FC4-32 port blades, FR4-18i FCIP blade and FC10-6 10 Gbit/sec port blade for ISL connections), SAN Switch 4/32, 4/64 SAN Switch and SAN Switch 4/32B switches. The 400 MP Router and FR4-18i blade (for the 4/256 SAN Director) provide FICON over IP extension. The 400 MP Router and FR4-18i blade (for the 4/256 SAN Director) also support direct FICON device switching in a single hop FICON configuration. The FC10-6 is supported for 10 Gbit/sec ISL links.

The following port blades can exist in a FICON environment; however, FICON device connection to ports on these blades is not supported:

- FC4-16IP
- FC4-48
- FC8-48

**NOTE:** The FC4-48 and FC8-48 port blades are not supported for connecting to System z environments through FICON channels or through FCP zLinux on System z.

In an Admin Domain-enabled fabric, you should put all of the ports on the FC4-48, FC8-48, and FC4-16IP blades in an Admin Domain other than the one used for FICON ports. The ports on these blades should not belong to the zone in which FICON devices are present.

The port-based routing policy is required in either in a single-switch configuration, or a cascaded switch configuration on switches in the fabric that have FICON devices attached (option 1 of the aptPolicy command). Other switches in the fabric can use the default exchange-based routing policy (option 3 of the aptPolicy command) only when Open Systems devices are attached to those switches.

**Types of FICON configurations**

There are two types of FICON configurations:

- A *single-switch* configuration (called *switched point-to-point*) requires that the channel be configured to use single-byte addressing. If the channel is set up for two-byte addressing, then the cascaded configuration setup applies. This type of configuration is described in “Configuring a single switch” on page 267.

- A *cascaded configuration* (known as a *high integrity fabric*) requires a list of authorized switches. This authorization feature, called *fabric binding* is available through the Secure Access Control List feature. The fabric binding policy allows a predefined list of switches (domains) to exist in the fabric and prevents other switches from joining the fabric. This type of configuration is described in “Configuring a high-integrity fabric” on page 267.

**Control Unit Port (CUP)**

**IMPORTANT:** HP highly recommends installing and enabling CUP.

Control Unit Port (CUP) protocol is used by IBM mainframe management programs to provide in-band management for FICON switches. When it is enabled, you can set up directors in a FICON environment to be managed through IBM mainframe management programs. CUP is an optional licensed feature.

The following restrictions apply to FICON directors having at least 256 ports when FICON Management Server mode (fmsmode) is enabled and CUP protocol is used to manage the switch:

- The switch is advertised to the mainframe by CUP as a 256-port switch (due to CUP protocol limitation).
- Port Information Block, PDCM, and port names are available for ports 0 through 254 only.
- CUP is not supported on the FC4-48 port blade. Even though the FC4-48 port blade can be inserted in the chassis, only FCP ports can be attached to it.
The FR4-18i routing blade must not be inserted in slot 10 of the chassis. (Other blades are supported in slot 10, but the FR4-18i blade is not.) FICON channels and control units can be attached only to the FC ports on this blade. This blade is advertised to the mainframe as a 16-port blade. If you have an FC4-18i blade in slot 10 in your director, the 16 virtual ports are disabled when you enable fmsmode.

The FC4-48 and FC8-48 port blades must not be inserted in slot 10 of the chassis in a FICON configuration. (Other blades are supported in slot 10, but the FC8-48 and FC4-48 blades are not.) Port 255 is reserved for CUP.

### FICON commands

Table 61 summarizes the Fabric OS CLI commands that can be used for managing FICON fabrics. For detailed information on these commands, see the *Fabric OS Command Reference*.

Table 61  Fabric OS commands related to FICON and FICON CUP

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Fabric OS commands</strong></td>
<td></td>
</tr>
<tr>
<td>configure</td>
<td>Sets the Domain ID and the insistent Domain ID mode.</td>
</tr>
<tr>
<td>portSwap</td>
<td>Swaps ports.</td>
</tr>
<tr>
<td>portSwapDisable</td>
<td>Disables the portSwap command.</td>
</tr>
<tr>
<td>portSwapEnable</td>
<td>Enables the portSwap command.</td>
</tr>
<tr>
<td>portSwapShow</td>
<td>Displays information about swapped ports.</td>
</tr>
<tr>
<td><strong>Commands specific to FICON</strong></td>
<td></td>
</tr>
<tr>
<td>ficonclear rlir</td>
<td>Removes all RLIR records from the local RLIR database.</td>
</tr>
<tr>
<td>ficonclear rnid</td>
<td>Removes all outdated RNID records from the local RNID database.</td>
</tr>
<tr>
<td>ficonshow ilir [fabric]</td>
<td>Displays FRU failure information on the local switch or on the fabric.</td>
</tr>
<tr>
<td>ficonshow lirr [fabric]</td>
<td>Displays registered listeners for link incidents for the local switch or for the fabric.</td>
</tr>
<tr>
<td>ficonshow rlir [fabric]</td>
<td>Displays link incidents for the local switch or for the fabric.</td>
</tr>
<tr>
<td>ficonshow rnid [fabric]</td>
<td>Displays node identification data for all devices registered with the local switch or all devices registered with all switches defined in the fabric.</td>
</tr>
<tr>
<td><strong>Commands specific to FICON CUP:</strong></td>
<td></td>
</tr>
<tr>
<td>ficoncupset fmsmode</td>
<td>Sets FICON Management Server mode on or off for the switch.</td>
</tr>
<tr>
<td>ficoncupset modereg</td>
<td>Sets the mode register bits for the switch.</td>
</tr>
<tr>
<td>ficoncupshow fmsmode</td>
<td>Displays the FICON Management Server mode setting for the switch.</td>
</tr>
<tr>
<td>ficoncupshow modereg</td>
<td>Displays the mode register bit settings for the switch.</td>
</tr>
</tbody>
</table>

**NOTE:** The Fabric OS CLI supports only a subset of the management features for FICON fabrics. The full set of FICON CUP administrative procedures is available using the Fabric Manager and Web Tools software features. You can also use an SNMP agent and the FICON Management Information Base (MIB).
For information on these tools, see:

- Web Tools—Web Tools Administrator’s Guide
- Fabric Manager—Fabric Manager Administrator’s Guide
- SNMP Agent and FICON Management Information Base (MIB)—Fabric OS MIB Reference

User security considerations

To administer FICON, you must have one of the following roles:

- Admin
- Operator
- SwitchAdmin
- FabricAdmin

The User and BasicSwitchAdmin roles are view-only. The ZoneAdmin and SecurityAdmin roles have no access.

In an Admin Domain-aware fabric, if you use the FICON commands (ficonshow, ficonclear, ficoncupshow, and ficoncupset) for any Admin Domain other than AD0 and AD255, the current switch must be a member of that Admin Domain. The output is not filtered based on the Admin Domain.

Configuring switches

Use the worksheet on page 278 to record your configuration information.

Following are recommended FICON environment configuration settings:

- Disable dynamic load sharing (dlsReset command).
  
  If DLS is enabled, traffic on existing ISL ports might be affected when one or more new ISLs is added between the same two switches. Specifically, adding the new ISL might result in dropped frames as routes are adjusted to take advantage of the bandwidth provided. By disabling DLS, you ensure that there will be no dropped frames.

  A similar situation occurs when an ISL port is taken offline and then brought back online. When the ISL port goes offline, the traffic on that port is rerouted to another ISL with a common destination. When the ISL port comes back online and DLS is enabled, the rerouting of traffic back to the ISL port might result in dropped frames. If DLS is not enabled, traffic is not routed back.

- Configure ports that are connected to 1 Gbps channels for fixed 1-Gbps speed. Otherwise, when using fixed 1-Gbps channels (both G5 and FICON Express), the FICON host might generate erroneous link incidents when the channels are coming online. These link incidents will result in a call home. Other than the generated link incident, the channel will come online and function normally.

- Use the port-based routing policy on any switch that has FICON devices attached. Other switches in the fabric with Open Systems devices exclusively can still use exchange-based routing.

- Enable in-order delivery (iodSet command).

- If you have any Extended Fabrics links, enable VC translation link initialization to stabilize them. See “Administering Extended Fabrics” on page 117 for details on this option of the portCfgLongDistance command.

- Follow standard FCP zoning practices even though there are no specific zoning rules related to FICON environments. For management purposes, when operating in a mixed environment put FCP devices in one zone and FICON devices in another zone.

- Configure ports for fixed 1 Gbps speed when there are 1 Gbps devices attached to them and those devices cannot auto-negotiate speed.
Preparing a switch

To verify and prepare a switch for use in a FICON environment, complete the following steps:

1. Connect to the switch and log in as admin.
2. Enter the `switchShow` command to verify that the switch and devices are online.
3. Change the routing policy on the switch from the default exchange-based policy to the required port-based policy for those switches with FICON devices directly attached using the `aptPolicy` command when working from the command line. For GUI-based procedures, see the Web Tools Administrator’s Guide for configuring the routing policy using the FICON tab in Web Tools.
4. Enter the `ficonshow rnid` command to verify that the FICON devices are registered with the switch.
5. Enter the `ficonshow lirr` command to verify that the FICON host channels are registered to listen for link incidents.
6. Optionally, see “Using FICON CUP” on page 270 for details about using FICON CUP.

Configuring a single switch

Single-switch configuration does not require IDID or fabric binding, provided that connected channels are configured for single-byte addressing. However, you should configure IDID to ensure that Domain IDs are maintained.

Configuring a high-integrity fabric

To configure a high-integrity fabric (cascaded configuration):

1. Disable each switch in the fabric.
2. For each switch:
   a. Enable the IDID flag.
   b. Set the Domain ID.
3. Enable the switches; this builds the fabric.
4. Set the SCC policy, as described in “Configuring advanced security features” on page 17.
5. Configure the Switch Connection Control policies on all switches to limit connectivity to only the switches in the selected fabric using the `secPolicyCreate` command.

```
switch:admin> secPolicyCreate SCC_POLICY, member;...;member
```

Where:

- `member` indicates a switch that is permitted to join the fabric. Specify switches by WWN, Domain ID, or switch name. Enter an asterisk (*) to indicate all the switches in the fabric. To create a policy that includes all the switches in the fabric:

```
switch:admin> secPolicyCreate SCC_POLICY "*"
```
6. Save or activate the new policy, enter either the `secPolicySave` or the `secPolicyActivate` command. If neither of these commands is entered, the changes are lost when the session is logged out. To activate the SCC policy:

```
switch:admin> secPolicyActivate
```
7. Enable ACL Fabric Wide Consistency Policy and enforce a strict SCC policy:

```
switch:admin> fddcfg --fabwideset "SCC:S"
```
8. Connect and enable channel and control unit (CU) devices. The Query for Security Attributes (QSA) response to the channel indicates that the fabric binding and IDID are enabled.
**Figure 19** and **Figure 20** show two viable cascaded configurations. These configurations require Channel A to be configured for two-byte addressing and require IDID and fabric binding. It is recommended that there are only 2 domains in a path from a FICON Channel interface to a FICON Control Unit interface.

**Figure 19** Cascaded configuration, two switches

**Figure 20** Cascaded configuration, three switches

### Setting a unique Domain ID

In a cascaded configuration, each switch must have a unique Domain ID, and insistent Domain ID (IDID) mode must be enabled.

To set a unique Domain ID and enable IDID mode:

1. Connect to the switch and log in as admin.
2. Verify that the switch has a unique Domain ID. If it does not, set a unique Domain ID.
   
   For instructions on displaying and changing the Domain ID, see “Working with domain IDs” on page 36.
3. Enter the `switchDisable` command to disable the switch.
4. Enter the `configure` command.
5. Enter `y` after the Fabric Parameters prompt.
6. To enable IDID mode, enter `y` after the “Insistent Domain ID Mode” prompt.
   
   You can disable this mode by entering `n`.
7. Respond to the remaining prompts (or press Ctrl-d to accept the other settings and exit).
8. Enter the `switchEnable` command to re-enable the switch.

   switch:admin> configure
   Configure...
   Fabric parameters (yes, y, no, n): [no] yes
   Domain: (1..239) [3] 5
   R_A_TOV: (4000..120000) [10000]
   E_D_TOV: (1000..5000) [2000]
   Data field size: (256..2112) [2112]
   Sequence Level Switching: (0..1) [0]
   Disable Device Probing: (0..1) [0]
   Suppress Class F Traffic: (0..1) [0]
   VC Encoded Address Mode: (0..1) [0]
   Per-frame Route Priority: (0..1) [0]
   Long Distance Fabric: (0..1) [0]
   BB credit: (1..16) [16]
   Insistent Domain ID Mode (yes, y, no, n): [no] y
   Virtual Channel parameters (yes, y, no, n): [no]
   Switch Operating Mode (yes, y, no, n): [no]
   Zoning Operation parameters (yes, y, no, n): [no]
   RSCN Transmission Mode (yes, y, no, n): [no]
   Arbitrated Loop parameters (yes, y, no, n): [no]
   System services (yes, y, no, n): [no]
   Portlog events enable (yes, y, no, n): [no]
   Committing configuration...done.
   switch:admin>

Displaying information

You can display link incidents, registered listeners, node identification data, and FRU failures, as described in the following procedures.

Link incidents

The registered link incident record (RLIR) ELS contains the link incident information sent to a listener N_Port.

To display link incidents, connect to the switch, log in as user, and enter one of the following commands:

- For the local switch: `ficonshow rlir`
- For all switches defined in the fabric: `ficonshow rlir fabric`

Registered listeners

To display registered listeners for link incidents, connect to the switch, log in as user, and enter one of the following commands:

- For the local switch: `ficonshow lirr`
- For all switches defined in the fabric: `ficonshow lirr fabric`

Node identification data

To display node-identification data, connect to the switch, log in as user, and enter any of the following commands:

- For the local switch: `ficonshow switchrnid`
- For all switches defined in the fabric: `ficonshow switchrnid fabric`
- For all devices registered with the local switch: `ficonshow rrid`
- For all devices registered with all switches defined in the fabric: `ficonshow rrid fabric`

FRU failures

To display FRU failure information, connect to the switch, log in as admin, and enter one of the following commands:

- For the local switch: `ficonshow ilir`
- For all switches defined in the fabric: `ficonshow ilir fabric`
Swapping ports
If a port malfunctions, or if you want to connect to different devices without having to re-wire your infrastructure, you can move a port’s traffic to another port (swap ports) without changing the I/O Configuration Data Set (IOCDS) on the mainframe computer.

To swap ports:
1. Connect to the switch and log in as admin.
2. Enter the portSwapEnable command (to enable the command for port swapping).
3. Enter the portDisable command to disable the two ports to be swapped.
4. Enter the portSwap command to swap the ports.
   Any port in the switch can be used as the alternate for any other port within the same switch.
5. Re-enable the ports using the portEnable command.
6. Enter portSwapDisable (to disable the command for port swapping).

In the following example:

```
switch:admin> portswapenable
switch:admin> portdisable [slot/] portA [slot/]portB
switch:admin> portswap [slot/] portA [slot/]portB
switch:admin> portenable [slot/] portA [slot/]portB
switch:admin> portswapdisable
```

- slot is the slot number of the port blade for a system with port blades (optional).
- portA is the original port number.
- portB is the alternate port number.

You can use the portSwapShow command to display information about swapped ports in a switch.

You can use the portSwap command to disable the portswap feature. You cannot use the portSwap command after this feature is disabled. The enabled state of the portswap feature is persistent across reboots and power cycles. Enabling and disabling the portswap feature does not affect previously executed portswap operations.

See the Fabric OS Command Reference for additional details about the portSwap command.

Clearing the FICON management database
Perform the following steps to clear RLIR and RNID records from the FICON management database.

1. Connect to the switch and log in as admin.
2. To remove all the RLIR records from the local RLIR database, enter ficonclear rlir.
3. To remove all the RNID records marked “not current” from the local RNID database, enter ficonclear rni.

Using FICON CUP
Host-based management programs manage switches using CUP protocol by sending commands to an emulated control device in the Fabric OS. An HP StorageWorks switch that supports CUP can be controlled by one or more host-based management programs or the Fabric OS tools provided by HP.

A mode register controls the behavior of the switch with respect to CUP itself, and with respect to the behavior of other management interfaces.

FICON Management Server mode (fmsmode) must be enabled on the switch to enable CUP management features. When this mode is enabled, Fabric OS prevents local switch commands from interfering with host-based management commands by initiating serialized access to switch parameters.

If Advanced Zoning is in use, see “Zoning and PDCM considerations” on page 275.
Setup summary

To set up FICON CUP, use the following procedure and be sure to perform the steps in the order indicated.

1. For directors with at least 256 ports installed, use the PortDisable command to disable (block) ports 254 and 255.
   Ports 254 and 255 are not supported in a CUP environment. After fmsmode has been successfully enabled, these two ports remain disabled and cannot be used either as an F_Port or an E_Port. Because these ports are not available after enabling fmsmode, you should first move any fiber connected to either of them to another free port.

2. Install a CUP license on the switch. See “Acquiring licensed features” on page 33.


After completing the setup, you can configure CUP attributes (FMS parameters). See ”Setting mode register bits” on page 274.

Enabling and disabling FICON Management Server mode

To enable fmsmode:

1. Connect to the switch and log in as admin.
2. Enter `ficoncupset fmsmode enable`.

To disable fmsmode:

1. Connect to the switch and log in as admin.
2. Enter `ficoncupset fmsmode disable`.

The fmsmode setting can be changed whether the switch is offline or online. If fmsmode is changed while the switch is online, a device reset is performed for the control device and an RSCN is generated with PID 0xDDFE00 (where 0xDD is the Domain ID of the switch).

When FICON Management Server mode is on, the Fabric OS CLI commands listed next return a “switch busy” response if they are issued when the host-based management tool is performing a write operation. This serialization prevents interference from local switch commands when a host-based management program is being used to administer the switch.

```
bladeDisable  bladeEnable
bladeEnable  bladeDisable
portDisable  switchCfgPersistentEnable
             switchCfgPersistentDisable
portEnable   switchDisable
portName     switchEnable
portShow     switchName
portSwap     switchShow
```

**NOTE:** You cannot use the `portCfgPersistentEnable` and `portCfgPersistentDisable` commands to persistently enable and disable ports when FICON Management Server mode is on. See the procedure “Persistently enabling/disabling ports” on page 274 for instructions.

Changing fmsmode from `disabled` to `enabled` triggers the following events:

- Access to switch parameters is serialized.
- The active CUP configuration data is established as follows:
  - Port and switch names are not read from the IPL; they remain as previously set.
  - Port “Block” and “Unblock” values are not read from the IPL; they remain as previously set with the `portEnable` and `portDisable` commands.
  - PDCM values are read from the IPL; the default is “Allow All.”
• Advanced Zoning, if used, continues to be in force. If there are any differences in restrictions set up with Advanced Zoning and PDCM, the most restrictive rules are automatically applied.
• RSCNs are sent to devices if PDCM results in changes to connectivity between a set of ports.

Changing fmsmode from enabled to disabled triggers the following events:
• A device reset is performed on the control device.
• PDCM is no longer enforced.
• RSCNs might be generated to some devices if PDCM removal results in changes to connectivity between a set of ports.
• If a given port was set to “Block” or “Unblock,” that port remains disabled or enabled.
• Serialized access to switch parameters ceases.

Setting up CUP when FICON Management Server mode is enabled

When a CUP license is installed, the transition from fmsmode disabled to fmsmode enabled triggers notification to the host systems that the CUP feature is available. Without this notification, the host systems never know that the CUP feature is available and, consequently, never try to communicate with it.

If you install a CUP license on a switch that already has fmsmode enabled, you must disable fmsmode first and reenable it after the license is installed so the host systems get the notification that CUP is enabled.

To set up FICON CUP if fmsmode is already enabled:
1. Verify that FICON Management Server mode is enabled by entering the `ficoncupshow fmsmode` command.

   **NOTE:** If fmsmode is already enabled, disabling it might be disruptive to operation because ports that were previously prevented from communicating will now be able to do so.

2. If FICON Management Server mode is enabled, then disable it by entering the `ficoncupset fmsmode disable` command.
   Install a CUP license key as described in “Adding and removing FICON CUP licenses” on page 275.
3. Enter the `ficoncupset fmsmode enable` command.

Displaying the fmsmode setting

The `ficoncupshow fmsmode` command displays the effective fmsmode setting for the switch.

```
switch:admin> ficoncupshow fmsmode
fmsmode for the switch: Enabled
```
Displaying mode register bit settings

The mode register bits are described in Table 62.

**Table 62** FICON CUP mode register bits

<table>
<thead>
<tr>
<th>POSC</th>
<th>Programmed offline state control. When this bit is set on, the host is prevented from taking the switch offline. The default setting is 1 (on).</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAM</td>
<td>User alert mode. When this bit is set on, a warning is issued when an action is attempted that will write CUP parameters on the switch. The default setting is 0 (off).</td>
</tr>
<tr>
<td>ASM</td>
<td>Active=saved mode. When this bit is set on, all CUP configuration parameters are persistent, meaning that they will be saved in nonvolatile storage in the initial program load (IPL) file that is applied upon a cold reboot or a power cycle. The default setting is 1 (on).</td>
</tr>
<tr>
<td>DCAM</td>
<td>Switch clock alert mode. When this bit is set on, a warning is issued when the <code>date</code>, <code>tsClockServer</code>, or <code>tsTimeZone</code> commands are entered to set the time and date on the switch. The default setting is 0 (off).</td>
</tr>
<tr>
<td>ACP</td>
<td>Alternate control prohibited. Because the Fabric OS CLI, Web Tools, and Fabric Manager are considered to be switch consoles, this bit has no effect on their operation. Attempts to set CUP parameters through SNMP are denied when this bit is set on. The default setting is 1 (on).</td>
</tr>
<tr>
<td>HCP</td>
<td>Host control prohibited. When this bit is set on, the host is not allowed to set CUP parameters. The default setting is 0 (off).</td>
</tr>
</tbody>
</table>

The `ficoncupshow modereg` command displays the mode register bit settings for the switch. A display of 0 indicates that the mode register bit is set to off; 1 indicates that the bit is set to on.

The command format is:

```
ficoncupshow modereg [bitname]
```

where `bitname` is one of the mode register bits described in Table 62.

To display all mode register bit settings for the switch:

```
switch:admin> ficoncupshow modereg
POSU AM   ASM   DCAM  ACP   HCP
---------------------
1 0 1 0 1 0
```

To display the mode register bit HCP for the switch:

```
switch:admin> ficoncupshow modereg HCP
HCP
0
```
Setting mode register bits

Use the `ficoncupset modereg` command to set the FICON CUP mode register bits for the local switch. Consider the following when changing mode register bits:

- As required by the CUP protocol, the UAM bit cannot be changed using this command.
- All mode register bits except UAM are saved across power on/off cycles; the UAM bit is reset to 0 following a power-on.
- Mode register bits can be changed when the switch is offline or online. If the ACP or HCP bits are changed when the switch is online, they will take effect any time between the completion of the current command and the end of the CCW command chain (or the next alternate manager operation).

The command format is:

```
ficoncupset modereg [byname] 0 | 1
```

where:

- `byname` One of the mode register bits described in "FICON CUP mode register bits" on page 273.
- 0 Specifies that the bit is off.
- 1 Specifies that the bit is on.

The following example sets the mode register bit HCP to off:

```
switch:admin> ficoncupset modereg HCP 0
Mode register bit HCP has been set to 0.
```

The following example sets the mode register bit ACP to on:

```
switch:admin> ficoncupset modereg ACP 1
Mode register bit ACP has been set to 1.
```

Persistently enabling/disabling ports

When fmsmode is enabled, you cannot use the `portCfgPersistentEnable` and `portCfgPersistentDisable` commands to persistently enable and disable ports. Instead, use the following procedure.

1. Enter the `ficoncupshow modereg` command to display the mode register bit settings.
2. Verify that the ASM bit is set on (1).
3. If the ASM bit is set off (0), enter the `ficoncupset modereg asm 1` command to set it on.
4. Use the `portEnable` and `portDisable` commands to enable and disable ports as necessary. The ports remain enabled or disabled after a switch reboot.

In the following example, the ASM bit is set to on; then, the port at slot 1, port 1 is enabled persistently:

```
switch:admin> ficoncupshow modereg
POSC  UAM  ASM  DCAM  ACP  HCP
-----------------------------
1    0 0 0    1 1

switch:admin> ficoncupset modereg ASM 1
Mode register bit ASM has been set to 1.

switch:admin> portenable 1/1
```
Port and switch naming standards

Fabric OS handles differences in port and switch naming rules between CUP and itself as follows:

- CUP employs 8-bit characters in port address names and switch names; Fabric OS employs 7-bit characters. When fmsmode is enabled, all characters greater than 0x40 and not equal to 0xFF (EBCDIC code page 37 [0x25]) are allowed in the name; therefore, it is possible for a channel to set a name with nonprintable characters. If a name contains nonprintable characters, they are displayed as dots (...). The following characters are also displayed as dots: semicolon (;), comma (,), equal sign (=), and at sign (@).

**NOTE:** Configuration files that contain nonprintable characters should not be edited manually because many editors replace nonprintable characters with some other characters without warning you first.

- CUP has a 24-character unique port name limitation; Fabric OS supports port names up to 32 characters long. When fmsmode is enabled, names longer than 24 characters are truncated.

- To ensure that they are unique, the characters ~00, ~01, ~02, and so on are appended to port names.

- CUP allows a 24-character switch name; Fabric OS limits the switch name to 15 characters. To reconcile this difference, Fabric OS files the first 15 characters in the WWN record and stores the extra characters for CUP use.

Adding and removing FICON CUP licenses

If fmsmode is enabled when the FICON CUP license is removed, the control device is reset. PDCM enforcement continues. If fmsmode is disabled when the FICON CUP license is removed, no special action is taken.

If fmsmode is enabled on a switch that does not have a FICON CUP license and then the license is installed, you must first disable and then reenable fmsmode. If fmsmode is disabled and a FICON CUP license is installed, no special action is required.

Zoning and PDCM considerations

The FICON Prohibit Dynamic Connectivity Mask (PDCM) controls whether or not communication between a pair of ports in the switch is prohibited or allowed. If there are any differences in restrictions set up with Advanced Zoning and PDCM, the most restrictive rules are automatically applied.

All FICON devices should be configured in a single zone using the “Domain, Area” notation. PDCM can then be used to “Allow” or “Prohibit” access between specific port pairs.

PDCM persists across a failover because it is replicated at all times to the standby CP blade. The active PDCM configuration is saved to the IPL if the ASM bit is set on.

Zoning and link incident reporting

Non-implicit link incidents (such as NOS recognized or bit error rate threshold exceeded) that are related to a specific port are reported to registered listeners only if they are in the same zone as the port for which the link incident is being reported. As long as all FICON devices are in a single zone, link incidents for FICON ports are reported only to registered FICON listener ports.

The only exception to this is the *loss of synchronization* link incident. Even though this link incident is related to a specific port, it can be reported to a registered listener that is in a different zone.

Implicit link incidents (such as WWN card failure or power supply failure) that are not related to a specific port are reported to registered listeners regardless of zoning configuration.
Troubleshooting

The following sources provide useful problem-solving information:

- The standard support commands (portLogDump, supportSave, supportShow) or the Fabric Manager Event log.

By default, the FICON group in the supportShow output is disabled. To enable the capture of FICON data in the supportShow output, enter the supportshowcfgenable ficon command. After you get confirmation that the configuration has been updated, the following will be collected and appear in the output for the supportShow command:

  - ficoncupshow fmsmode
  - ficoncupshow modereg
  - ficondbg dump rnid
  - ficondbg log
  - ficonshow ilir
  - ficonshow lirr
  - ficonshow rlir
  - ficonshow rnid
  - ficonshow switchrnid
  - ficucmd dump -A

- Other detailed information for protocol-specific problems:
  - Display port data structures using the ptDataShow command.
  - Display port registers using the ptRegShow command.

Identifying ports

The ficonshow rlir command displays, among other information, a tag field for the switch port. You can use this tag to identify the port on which a FICON link incident occurred. The tag field is a concatenation of the switch Domain ID and port number, in hexadecimal format. The following example shows a link incident for the switch port at Domain ID 120, port 93 (785d in hex):

```
switch:admin> ficonshow rlir
{Fmt  Type PID    Port   Incident Count  TS Format   Time Stamp
0x18 F    785d00   93                1  Time server Thu Apr 22 09:13:32 2004
Port Status:        Link not operational
Link Failure Type:   Loss of signal or synchronization
Registered Port WWN  Registered Node WWN      Flag  Node Parameters
50:05:07:64:01:40:16:03 50:05:07:64:00:c1:69:ca  0x10  0x200115
Type number:         002064
Model number:        103
Manufacturer:        IBM
Plant of Manufacture:02
Sequence Number:     0000000169CA
tag:                  155d
Switch Port WWN       Switch Node WWN          Flag  Node Parameters
20:5d:00:60:69:80:45:7c 10:00:00:60:69:80:45:7c  0x00  0x200a5d
Type number:         SLKWRM
Model number:        24K
Manufacturer:        BRD
Plant of Manufacture: CA
Sequence Number:     000000000078
tag:                  785d
}
```

The Local RLIR database has 1 entry.
Back up and restore FICON configuration files

The FICON file access facility is used to store configuration files. This includes IPL and other configuration files. The Fabric OS saves the IPL and all other configuration files on the switch. A maximum of 16 configuration files, including the IPL file, are supported.

You can upload the configuration files saved on the switch to a management workstation using the `configUpload` command. If the switch loses the configuration due to a hardware failure or filesystem error, use the `configDownload` command to restore previously uploaded configuration files. Because data uploaded using the `configUpload` command also contains the IPL, if Active=Saved mode is enabled, then the switch will ignore the IPL file downloaded with the `configDownload` command.

To upload the configuration files:

Enter the `configUpload` command.

When you execute the `configUpload` command, all the files saved in the file access facility are uploaded to a management workstation (there is a section in the uploaded configuration file labeled “FICON_CUP” that exists in an encoded format).

To download configuration files with Active=Saved mode enabled:

Enter the `configDownload` command.

The contents of existing files saved on the switch, which are also present in the “FICON_CUP” section, are overwritten.

The files in the “FICON” section of the configuration file, which are not currently on the switch, are saved on the switch.

The IPL will not be replaced because Active=Saved mode is enabled. A warning message is displayed in the event log to warn users that the IPL will not be overwritten.

To download configuration files with Active=Saved mode disabled:

Enter the `configDownload` command.

The contents of existing files saved on the switch, which are also present in the “FICON_CUP” section, are overwritten.

The files in the “FICON” section of the configuration file, which are not currently on the switch, are saved on the switch.

The IPL is replaced because Active=Saved mode is disabled.
Recording configuration information

You can use the following worksheet for recording FICON configuration information.

Table 63  FICON configuration worksheet

<table>
<thead>
<tr>
<th>FICON® Switch Configuration Worksheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>FICON® Switch Manufacturer: ___________________ Type: _______ Model: ______ S/N: ______</td>
</tr>
<tr>
<td>HCD Defined Switch ID________ (Switch ID)</td>
</tr>
<tr>
<td>FICON® Switch Domain ID________ (Switch @)</td>
</tr>
<tr>
<td>Cascaded Directors No ____ Yes ____</td>
</tr>
<tr>
<td>Corresponding Cascaded Switch Domain ID _____</td>
</tr>
<tr>
<td>Fabric Name ________________________________</td>
</tr>
<tr>
<td>FICON® Switch F_Ports</td>
</tr>
<tr>
<td>Attached N_Ports / E_Ports (CU, CPC, or ISL)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Port Number</th>
<th>Port Address</th>
<th>Laser Type: LX / SX</th>
<th>Port Name</th>
<th>Node Type: CU / CHNL</th>
<th>Machine Type</th>
<th>Model</th>
<th>Serial Number</th>
<th>ISL</th>
<th>CU I/F</th>
<th>CPC</th>
<th>CHPID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Sample IOCP configuration file

The channel subsystem controls communication between a configured channel, the control unit, and the device. The I/O Configuration Dataset (IOCDS) defines the channels, control units, and devices to the designated logical partitions (LPARs) within the server; this is defined using the Input/Output Configuration Program (IOCP). The IOCP statements are typically built using the hardware configuration dialog (HCD). The interactive dialog is used to generate your Input/Output Definition File (IODF), invoke the IOCP program, and subsequently build your production IOCDS.

Each FICON director in a fabric must have a unique Domain ID and a unique switch ID. The switch ID used in the IOCP definitions can be any value between x'00' to x'FF'. The Domain ID range for directors is hex x'01' to x'EF' or decimal 1 to 239. When defining the switch IDs in the IOCP definitions, ensure that you use values within the FICON director’s range.

The switch ID has to be assigned by the user and must be unique within the scope of the definitions (IOCP and HCD).

The Domain ID is assigned by the manufacturer and can be customized to a different value. It must be unique within the fabric.

HP recommends that the switch ID (in IOCP or HCD) be set to the same value as the Domain ID of the FICON director, which is defined to the FICON director at installation time. This simplifies the configuration and reduces confusion by having a common designation across all definitions.

For more information on switch numbering, refer to the IBM publication FICON® Implementation Guide (SG24-6497-00).

In the following sample IOCP configuration file, the UNIT value for FICON CUP definitions is 2032 for any FICON director regardless of vendor or platform. All HP switches require UNIT=2032 for the CUP definition. All Domain IDs are specified in hex values in the IOCP (and not in decimal values); the Domain IDs in the example are for demonstration purposes only.

```plaintext
*------------------------------------------------------------------
* Brocade Domain_ID=61 (in hex)                                     *
*------------------------------------------------------------------
CNTLUNIT CUNUMBR=0D8,UNITADD=00,UNIT=2032,
 PATH=(50,51),
 LINK=(61FE,61FE)
IODEVICE ADDRESS=(0D8,1),CUNUMBR=0D8,UNIT=2032,STADET=Y,UNITADD=00
*------------------------------------------------------------------
CNTLUNIT CUNUMBR=0DB,UNITADD=00,UNIT=2032,
 PATH=(5A,5B),
 LINK=(25FE,25FE)
IODEVICE ADDRESS=(0DB,1),CUNUMBR=0DB,UNIT=2032,STADET=Y,UNITADD=00
*------------------------------------------------------------------
* Brocade Domain_ID=25 (in hex)                                     *
*------------------------------------------------------------------
CNTLUNIT CUNUMBR=0D9,UNITADD=00,UNIT=2032,
 PATH=(8A,8B),
 LINK=(22FE,22FE)
IODEVICE ADDRESS=(0D9,1),CUNUMBR=0D9,UNIT=2032,STADET=Y,UNITADD=00
*------------------------------------------------------------------
```
# Configuring the Distributed Management Server

This chapter provides information on enabling and disabling the platform services, configuring and controlling access to the Management Server database, and using the topology discovery feature.

## Introduction

The Fabric OS Distributed Management Server allows a SAN management application to retrieve information and administer interconnected switches, servers, and storage devices. The Management Server assists in the autodiscovery of switch-based fabrics and their associated topologies.

A client of the Management Server can find basic information about the switches in the fabric and use this information to construct topology relationships. The Management Server also allows you to obtain certain switch attributes and, in some cases, modify them. For example, logical names identifying switches can be registered with the Management Server.

The Management Server provides several advantages for managing a Fibre Channel fabric:

- It is accessed by an external Fibre Channel node at the well-known address FFFFFAh, so an application can access information about the entire fabric management with minimal knowledge of the existing configuration.
- It is replicated on every HP StorageWorks switch within a fabric.
- It provides an unzoned view of the overall fabric configuration. This fabric topology view exposes the internal configuration of a fabric for management purposes; it contains interconnect information about switches and devices connected to the fabric. Under normal circumstances, a device (typically an FCP initiator) queries the name server for storage devices within its member zones. Because this limited view is not always sufficient, the Management Server provides the application with a list of the entire name server database.

## Enabling and disabling the platform services

The Management Server is located at the Fibre Channel address FFFFFAh. All management services except platform services are enabled by default.

**NOTE:** The commands `msplMgmtActivate` and `msplMgmtDeactivate` are allowed only in AD0 and AD255.

To enable platform services:
1. Connect to the switch and log in as admin.
2. Enter the `msplMgmtActivate` command.
   ```
   switch:admin> msplmgmtactivate
   Request to activate MS Platform Service in progress......
   *Completed activating MS Platform Service in the fabric!
   ```

To disable platform services:
1. Connect to the switch and log in as admin.
2. Enter the `msplMgmtDeactivate` command.
3. Enter y to confirm the deactivation.

```
switch:admin> mspmgmtdeactivate
MS Platform Service is currently enabled.
This will erase MS Platform Service configuration
information as well as database in the entire fabric.
Would you like to continue this operation? (yes, y, no, n): [no] y
Request to deactivate MS Platform Service in progress......
*Completed deactivating MS Platform Service in the fabric!
```

Controlling access

You can use the **msConfigure** command to control access to the Management Server database.

An access control list (ACL) of WWN addresses determines which systems have access to the Management Server database. The ACL typically contains those WWNs of host systems that are running management applications.

If the list is empty (the default), the Management Server is accessible to all systems connected in-band to the fabric. For more access security, you can specify WWNs in the ACL so that access to the Management Server is restricted to only those WWNs listed.

The ACL is switch-based. Therefore, only hosts that are connected directly to the switch are affected by the ACL. A host that is somewhere else in the fabric and is connected to a switch with an empty ACL is allowed to access the Management Server.

To display the Management Server ACL:

1. Connect to the switch and log in as admin.
2. Enter the **msConfigure** command.
   The command becomes interactive.
3. At the select prompt, enter 1 to display the access list.
   A list of WWNs that have access to the Management Server is displayed.
   In the following example, the list is empty:

```
switch:admin> msconfigure
0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 1
MS Access list is empty.
0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [0] 0
done ...
```

To add a member to the ACL:

1. Connect to the switch and log in as admin.
2. Enter the **msConfigure** command.
   The command becomes interactive.
3. At the select prompt, enter 2 to add a member based on its port/node WWN.
4. Enter the WWN of the host to be added to the ACL.
5. At the prompt, enter 1 to display the access list so you can verify that the WWN you entered was added to the ACL.
6. After verifying that the WWN was added correctly, enter 0 at the prompt to end the session.
7. At the “Update the FLASH?” prompt, enter y.
8. Press Enter to update the nonvolatile memory and end the session.

```
switch:admin> msconfigure
0   Done
1   Display the access list
2   Add member based on its Port/Node WWN
3   Delete member based on its Port/Node WWN
select : (0..3) [1] 2
Port/Node WWN (in hex): [00:00:00:00:00:00:00:00] 20:00:00:20:37:65:ce:aa
 *WWN is successfully added to the MS ACL.
0   Done
1   Display the access list
2   Add member based on its Port/Node WWN
3   Delete member based on its Port/Node WWN
select : (0..3) [2] 1
MS Access List consists of (14): {
  20:00:00:20:37:65:ce:aa
  20:00:00:20:37:65:ce:bb
  20:00:00:20:37:65:ce:ff
  20:00:00:20:37:65:ce:11
  20:00:00:20:37:65:ce:22
  20:00:00:20:37:65:ce:33
  20:00:00:20:37:65:ce:44
  10:00:00:60:69:04:11:24
  10:00:00:60:69:04:11:23
  21:00:00:e0:8b:04:70:3b
  10:00:00:60:69:04:11:33
  20:00:00:20:37:65:ce:55
  20:00:00:20:37:65:ce:66
  00:00:00:00:00:00:00:00
}
0   Done
1   Display the access list
2   Add member based on its Port/Node WWN
3   Delete member based on its Port/Node WWN
select : (0..3) [1] 0
done ...
Update the FLASH?   (yes, y, no, n): [yes] y
*Successfully saved the MS ACL to the flash.
switch:admin>
```
To delete a member from the ACL:

1. Connect to the switch and log in as admin.
2. Enter the `msConfigure` command.
   The command becomes interactive.
3. At the select prompt, enter 3 to delete a member based on its port/node WWN.
4. At the prompt, enter the WWN of the member to be deleted from the ACL.
5. At the prompt, enter 1 to display the access list so you can verify that the WWN you entered was deleted from the ACL.
6. After verifying that the WWN was deleted correctly, enter 0 at the prompt to end the session.
7. At the “Update the FLASH?” prompt, enter `y`.
8. Press Enter to update the nonvolatile memory and end the session.

```
switch:admin> msconfigure
0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 3
Port/Node WWN (in hex): [00:00:00:00:00:00:00:00] 20:00:00:20:37:65:ce:aa
*WWN is successfully deleted from the MS ACL.
0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [2] 1
MS Access List consists of (13): {
  20:00:00:20:37:65:ce:aa
  20:00:00:20:37:65:ce:bb
  20:00:00:20:37:65:ce:ff
  20:00:00:20:37:65:ce:11
  20:00:00:20:37:65:ce:22
  20:00:00:20:37:65:ce:33
  10:00:00:60:69:04:11:24
  10:00:00:60:69:04:11:23
  21:00:00:e0:8b:04:70:3b
  10:00:00:60:69:04:11:33
  20:00:00:20:37:65:ce:55
  20:00:00:20:37:65:ce:66
}
0       Done
1       Display the access list
2       Add member based on its Port/Node WWN
3       Delete member based on its Port/Node WWN
select : (0..3) [1] 0
done ...
Update the FLASH? (yes, y, no, n): [yes] y
*Successfully saved the MS ACL to the flash.
switch:admin>
```
Configuring the server database

The Management Server database can be viewed or cleared. The command `msPlClearDB` is allowed only in AD0 and AD255.

To view the contents of the Management Server database:

1. Connect to the switch and log in as admin.
2. Enter the `msPlatShow` command.
The contents of the Management Server platform database are displayed.

```
switch:admin> msplatshow

Platform Name: [9] "first obj"
Platform Type: 5 : GATEWAY
Number of Associated M.A.: 1
Number of Associated Node Names: 1
Associated Node Names:
10:00:00:60:69:20:15:71

Platform Name: [10] "second obj"
Platform Type: 7 : HOST_BUS_ADAPTER
Number of Associated M.A.: 1
Associated Management Addresses:
Number of Associated Node Names: 1
Associated Node Names:
10:00:00:60:69:20:15:75
```

To clear the Management Server database:

1. Connect to the switch and log in as admin.
2. Enter the `msplClearDb` command.
3. Enter `y` to confirm the deletion.
The Management Server platform database is cleared.

Controlling topology discovery

The topology discovery feature can be displayed, enabled, and disabled; it is disabled by default. The commands `mstdEnable` and `mstdDisable` are allowed only in AD0 and AD255.

To display topology discovery status:

1. Connect to the switch and log in as admin.
2. Enter the `mstdReadConfig` command.
   ```
   switch:admin> mstdreadconfig
   *MS Topology Discovery is Enabled.
   ```

To enable topology discovery:

1. Connect to the switch and log in as admin.
2. Enter the `mstdEnable` command to enable the discovery feature locally.
3. Enter the `mstdEnable all` command to enable the discovery feature on the entire fabric.
   ```
   switch:admin> mstdenable
   ```
Request to enable MS Topology Discovery Service in progress....
*MS Topology Discovery enabled locally.

switch:admin> mstdenable ALL

Request to enable MS Topology Discovery Service in progress....
*MS Topology Discovery enabled locally.
*MS Topology Discovery Enable Operation Complete!!

To disable topology discovery:
1. Connect to the switch and log in as admin.
2. Enter the appropriate following command based on how you want to disable discovery:
   - For the local switch, enter the mstdDisable command.
   - For the entire fabric, enter the mstdDisable all command.
   A warning displays that all NID entries might be cleared.
3. Enter y to disable the discovery feature.

**NOTE:** Disabling discovery of Management Server topology might erase all NID entries.

switch:admin> mstddisable
This may erase all NID entries. Are you sure?  (yes, y, no, n): [no] y

Request to disable MS Topology Discovery Service in progress....
*MS Topology Discovery disabled locally.

switch:admin> mstddisable all
This may erase all NID entries. Are you sure?  (yes, y, no, n): [no] y

Request to disable MS Topology Discovery Service in progress....
*MS Topology Discovery disabled locally.
*MS Topology Discovery Disable Operation Complete!!
13 Working with Diagnostic Features

This chapter provides information on diagnostics and how to display system, port, and specific hardware information. It also describes how to set up system logging mapping (syslogd) and how to set up offloading error messages (supportSave).

About Fabric OS diagnostics

The purpose of the diagnostic subsystem is to evaluate the integrity of the system hardware.

Diagnostics are invoked in the following two ways:

- Automatically during the power-on self test (POST)
- Manually using Fabric OS CLI commands

The error messages generated during these test activities are sent to the serial console and system message logs, whose output formats may differ slightly.

Use the diagHelp command to receive a list of all available diagnostic commands.

See the Fabric OS Command Reference for a complete description of each command.

Viewing power-on self test

By default, when you power on the system, the boot loader automatically performs power-on self tests and loads a Fabric OS kernel image.

The POST tests provide a quick indication of hardware readiness when hardware is powered up. These tests do not require user input to function. They typically operate within several minutes, and support minimal validation because of the restriction on test duration. Their purpose is to give a basic health check before a new switch joins a fabric.

These tests are divided into two groups: POST1 and POST2. POST1 validates the hardware interconnect of the device, and POST2 validates the ability of the device to pass data frames between the ports. The specific set of diagnostic and test commands run during POST depends on the switch model.

The factory default configuration is set to run POST2, but you can configure your switch to bypass POST2, which runs after the kernel image has started but before general system services such as login are enabled.

Although each test performed during POST2 is configurable, you should only modify a POST2 test if directed by your switch provider’s customer service representative.

You can use the diagDisablePost command to disable both POST1 and POST2, and you can reenable it using the diagEnablePost command. See the Fabric OS Command Reference for additional information about these commands.

The following example shows a typical boot sequence, including POST messages:

```
The system is coming up, please wait...

Read board ID of 0x80 from addr 0x23
Read extended model ID of 0x16 from addr 0x22
Matched board/model ID to platform index 4
PCI Bus scan at bus 0
:::
:::
Checking system RAM - press any key to stop test

Checking memory address: 00100000

System RAM test using Default POST RAM Test succeeded.
```
Press escape within 4 seconds to enter boot interface.
Booting "Fabric Operating System" image.

Linux/PPC load:
BootROM command line: quiet
Uncompressing Linux... done.
Now booting the kernel
Attempting to find a root file system on hda2...
modprobe: modprobe: Can't open dependencies file
/lib/modules/2.4.19/modules.dep (No such file or directory)
INIT: version 2.78 booting
INIT: Entering runlevel: 3
eth0: Link status change: Link Up. 100 Mbps Full duplex Auto
  (autonegotiation complete).

INITCP: CPLD Vers: 0x95 Image ID: 0x19
uptime: 2008; sysc_qid: 0
Fabric OS (Paulsa45)
Paulsa45 console login: 2005/03/31-20:12:42, [TRCE-5000], 0,, INFO, ?,
trace:, trace_buffer.c, line: 1170

2005/03/31-20:12:42, [LOG-5000], 0,, INFO, SW4100_P45, Previous message
repeat 1 time(s), trace_ulib.c, line: 540
2005/03/31-20:12:43, [HAM-1004], 219,, INFO, SW4100_P45, Processor
rebooted - Unknown
SNMP Research SNMP Agent Resident Module Version 15.3.1.4
sysctrld: all services Standby
FSSK 2: chassis0(0): state not synchronized
FSSK 2: Services starting a COLD recovery
2005/03/31-20:12:48, [FSS-5002], 0,, INFO, SW4100_P45, chassis0(0): state
not synchronized, svc.c, line: 318
2005/03/31-20:12:48, [FSS-5002], 0,, INFO, SW4100_P45, Services starting a
COLD recovery, mdev.c, line: 638
2005/03/31-20:12:49, [MFIC-1002], 220,, INFO, Paulsa45, Chassis PRU header
not programmed for switch NID, using defaults (applies only to FICON
environments).
sysctrld: all services Active
2005/03/31-20:12:50, [DGD-5001], 0,, INFO, SW4100_P45, Slot 0 has started
POST., main.c, line: 1189
POST1: Started running Thu Mar 31 20:12:51 GMT 2005
POST1: Test #1 - Running turboramtest
POST1: Test #2 - Running portregtest
POST1: Script PASSED with exit status of 0 Thu Mar 31 20:12:54 GMT 2005
took (0:0:3)
POST2: Started running Thu Mar 31 20:12:55 GMT 2005
POST2: Test #1 - Running portloopbacktest (SERDES)
POST2: Test #2 - Running minicycle (SERDES)
POST2: Running diagshow
POST2: Script PASSED with exit status of 0 Thu Mar 31 20:13:12 GMT 2005 took (0:0:17)
2005/03/31-20:13:13, [BL-1000], 221,, INFO, Paulsa45, Initializing Ports... Enabling switch...
2005/03/31-20:13:13, [BL-1001], 222,, INFO, Paulsa45, Port Initialization Completed
2005/03/31-20:13:13, [EM-5012], 0,, INFO, SW4100_P45, EM: sent dumpready to ME., em.c, line: 2152
2005/03/31-20:13:13, [DGD-5002], 0,, INFO, SW4100_P45, Slot 0 has passed the POST tests., main.c, line: 936

If you choose to bypass POST2, or after POST2 completes, various system services are started and the boot process displays additional console status and progress messages.

**Viewing switch status**

Use the `switchStatusShow` command to display the overall status of the switch, including its power supplies, fans, and temperature. If the status of any one of these components is either marginal or down, the overall status of the switch is also displayed as marginal or down. If all components have a healthy status, the switch displays a healthy status.

To modify the rules used to classify the health of each component use the `switchStatusPolicySet` command. To view the rules, use the `switchStatusPolicyShow` command.

To view the overall status of the switch:

1. Connect to the switch and log in as admin.
2. Enter the `switchStatusShow` command:

```
switch:admin> switchstatusshow
Switch Health Report  Report time: 03/21/2005 03:50:36 PM
Switch Name:    SWFCR
IP address:     10.33.54.176
SwitchState:    MARGINAL
Duration:       863:23
Power supplies monitor  MARGINAL
Temperatures monitor   HEALTHY
Fans monitor        HEALTHY
WWN servers monitor  HEALTHY
Standby CP monitor   HEALTHY
Blades monitor      HEALTHY
Flash monitor       HEALTHY
Marginal ports monitor  HEALTHY
Faulty ports monitor  HEALTHY
Missing SFPs monitor  HEALTHY
All ports are healthy
```

For more information on how the overall switch status is determined, see the `switchStatusPolicySet` command in the *Fabric OS Command Reference*. 
To display switch information:

1. Connect to the switch and log in as admin.
2. Enter the `switchShow` command, which displays the following information for a switch:
   - `switchname`—The switch name.
   - `switchtype`—The switch model and firmware version numbers.
   - `switchstate`—The switch state: Online, Offline, Testing, or Faulty.
   - `switchrole`—The switch role: Principal, Subordinate, or Disabled.
   - `switchdomain`—The switch Domain ID.
   - `switchid`—The embedded port D_ID of the switch.
   - `switchwwn`—The switch World Wide Name.
   - `switchbeacon`—The switch beaconing state: either ON or OFF.

   The `switchShow` command also displays the following information for ports on the specified switch:
   - `Module type`—The SFP type if an SFP is present.
   - `Port speed`—The speed of the Port (1G, 2G, 4G, N1, N2, N4, or AN). The speed can be fixed, negotiated, or auto-negotiated.
   - `Port state`—The port status.
   - `Comment`—Information about the port. This section may be blank or display the WWN for an F_Port or an E_Port, the trunking state, or upstream or downstream status.

   The details displayed for each switch differ on different switch models. For more information see the `switchShow` command in the *Fabric OS Command Reference*.

To display the uptime for a switch:

1. Connect to the switch and log in as admin.
2. Enter the `uptime` command:

   ```
   switch:admin> uptime
   4:43am up 1 day, 12:32, 1 user, load average: 1.29, 1.31, 1.27
   switch:admin>
   ```

   The `uptime` command displays the length of time the system has been in operation, the total cumulative amount of uptime since the system was first powered-on, the date and time of the last reboot (applies only to Fabric OS 3.x and 2.6.x systems), the reason for the last reboot (applies only to Fabric OS 3.x and 2.6.x systems), and the load average over the past one minute (1.29 in the preceding example), five minutes (1.31 in the example), and 15 minutes (1.27 in the example). The reason for the last switch reboot is also recorded in the system message log.
Viewing port information

Use the following commands to view information about ports.

To view the status of a port:

1. Connect to the switch and log in as admin.
2. Enter the `portShow` command, specifying the number that corresponds to the port you are troubleshooting. In this example, the status of port two is shown:

```
switch:admin> switch:user> portshow 0

portName: 
portHealth: OFFLINE

Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x4001 PRESENT U_PORT LED
portType:  4.1
portState: 2   Offline
portPhys: 2   No_Module
portScn: 0
port generation number: 0
portId: 010000
portIfId: 43020020
portWwn: 20:00:00:60:69:00:02:53
portWwn of device(s) connected:

Distance: normal
portSpeed: N2Gbps

LE domain: 0
Interrupts: 0   Link_failure: 0   Frjt: 0
Unknown: 0   Loss_of_sync: 0   Fbsy: 0
Lli: 0   Loss_of_sig: 0
Proc_rqrd: 0   Protocol_err: 0
Timed_out: 0   Invalid_word: 0
Rx_flushed: 0   Invalid_crc: 0
Tx_unavail: 0   Delim_err: 0
Free_buffer: 0   Address_err: 0

Port part of other ADs: Yes
```

See the Fabric OS Command Reference for additional `portShow` command information, such as the syntax for slot or port numbering, displaying IP interfaces on a GbE port, or displaying FCIP tunnel connection or configuration information.
To display the port statistics:

1. Connect to the switch and log in as admin.
2. At the command line, enter the `portStatsShow` command.

Port statistics include information such as the number of frames received, number of frames sent, number of encoding errors received, and number of class 2 and class 3 frames received.

See the *Fabric OS Command Reference* for additional `portStatsShow` command information, such as the syntax for slot or port numbering.

```
switch:admin> portstatsshow 3/7
stat_wtx                0           4-byte words transmitted
stat_wrx                0           4-byte words received
stat_frx                0           Frames transmitted
stat_frx                0           Frames received
stat_c2_frx             0           Class 2 frames received
stat_c3_frx             0           Class 3 frames received
stat_lc_rx              0           Link control frames received
stat_mc_rx              0           Multicast frames received
stat_mc_to              0           Multicast timeouts
stat_mc_tx              0           Multicast frames transmitted
tim_rdy_pri             0           Time R_RDY high priority
tim_txcrd_z             0           Time BB credit zero
er_enc_in               0           Encoding errors inside of frames
er_crc                  0           Frames with CRC errors
er_trunc                0           Frames shorter than minimum
er_toolong              0           Frames longer than maximum
er_bad_eof              0           Frames with bad end-of-frame
er_enc_out              0           Encoding error outside of frames
er_bad_os               0           Invalid ordered set
er_c3_timeout           0           Class 3 frames discarded due to timeout
er_c3_dest_unreach      0           Class 3 frames discarded due to destination unreachable
er_other_discard        0           Other discards
er_crc_good_eof         0           Crc error with good eof
er_inv_arb              0           Invalid ARB
open                    0           loop_open
transfer                0           loop_transfer
opened                  0           FL_Port opened
starve_stop             0           tenancies stopped due to starvation
fl_tenancy              0           number of times FL has the tenancy
nl_tenancy              0           number of times NL has the tenancy
zero_tenancy            0           zero tenancy
```

switch:admin>
To display a summary of port errors for a switch:

1. Connect to the switch and log in as admin.
2. Enter the `portErrShow` command. See the Fabric OS Command Reference for additional portErrShow command information.

```bash
switch:admin> porterrshow
frames  enc  crc  too too  bad  enc disc link loss loss frjt fbsy
  tx   rx   in  err shrt long  eof  out  c3 fail sync sig
sig===============================================
0:  22  24  0  0  0  0  0  1.5m  0  7  3  0  0  0
1:  22  24  0  0  0  0  0  1.2m  0  7  3  0  0  0
2:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
3:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
4: 149m 99m  0  0  0  0  0  448  0  7  6  0  0  0
5: 149m 99m  0  0  0  0  0  395  0  7  6  0  0  0
6: 147m 99m  0  0  0  0  0  706  0  7  6  0  0  0
7: 150m 99m  0  0  0  0  0  160  0  7  5  0  0  0
8:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
9:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
10:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
11:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
12:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
13:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
14:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
15:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
32:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
33:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
34:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
35:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
36:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
37:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
38:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
39:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
40:  99m 146m  0  0  0  0  0  666  0  6  796  7  0  0
41:  99m 149m  0  0  0  0  0  15k  0  2  303  4  0  0
42:  99m 152m  0  0  0  0  0  665  0  2  221  5  0  0
43:  99m 147m  0  0  0  0  0  16k  0  2  144  4  0  0
44:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
45:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
46:  0  0  0  0  0  0  0  0  0  0  0  0  2  0  0
47:  0  0  0  0  0  0  0  0  0  0  0  0  0  0
```
The `portErrShow` command output provides one output line per port. See Table 64 for a description of the error types.

**Table 64   Error summary description**

<table>
<thead>
<tr>
<th>Error type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frames tx</td>
<td>Frames transmitted</td>
</tr>
<tr>
<td>frames rx</td>
<td>Frames received</td>
</tr>
<tr>
<td>enc in</td>
<td>Encoding errors inside frames</td>
</tr>
<tr>
<td>crc err</td>
<td>Frames with CRC errors</td>
</tr>
<tr>
<td>too shrt</td>
<td>Frames shorter than minimum</td>
</tr>
<tr>
<td>too long</td>
<td>Frames longer than maximum</td>
</tr>
<tr>
<td>bad eof</td>
<td>Frames with bad end-of-frame delimiters</td>
</tr>
<tr>
<td>enc out</td>
<td>Encoding error outside of frames</td>
</tr>
<tr>
<td>disc c3</td>
<td>Class 3 frames discarded</td>
</tr>
<tr>
<td>link fail</td>
<td>Link failures (LF1 or LF2 states)</td>
</tr>
<tr>
<td>loss sync</td>
<td>Loss of synchronization</td>
</tr>
<tr>
<td>loss sig</td>
<td>Loss of signal</td>
</tr>
<tr>
<td>frjt</td>
<td>Frames rejected with F_RJT</td>
</tr>
<tr>
<td>fbsy</td>
<td>Frames busied with F_BSY</td>
</tr>
</tbody>
</table>
Viewing equipment status

You can display status for fans, power supply, and temperature.

*NOTE:* The number of fans, power supplies, and temperature sensors depends on the switch type. For detailed specifications on these components, refer to the switch hardware reference manual. The specific output from the status commands varies depending on the switch type.

To display the status of the fans:

1. Connect to the switch and log in as admin.
2. Enter the `fanShow` command:

   ```
   switch:admin> fanshow
   Fan 1 is OK speed is 7010 RPM
   Fan 2 is OK speed is 7180 RPM
   Fan 3 is OK speed is 7068 RPM
   Fan 4 is OK speed is 7116 RPM
   Fan 5 is OK speed is 7155 RPM
   Fan 6 is OK speed is 7001 RPM
   switch:admin>
   ```

   The possible status values are:
   - OK—Fan is functioning correctly.
   - Absent—Fan is not present.
   - Below minimum—Fan is present but rotating too slowly or stopped.
   - Above minimum—Fan is rotating too quickly.
   - Unknown—Unknown fan unit installed.
   - FAULTY—Fan has exceeded hardware tolerance.

To display the status of a power supply:

1. Connect to the switch and log in as admin.
2. Enter the `psShow` command:

   ```
   switch:admin> psshow
   Power Supply #1 is OK
   0335,FF2Z0007161,60-0000739-02, B,,DCJ3002-01P, B,FF2Z0007161
   Power Supply #2 is faulty
   0335,FF2Z0007176,60-0000739-02, B,,DCJ3002-01P, B,FF2Z0007176
   switch:admin>
   ```

   The possible status values are:
   - OK—Power supply functioning correctly.
   - Absent—Power supply not present.
   - Unknown—Unknown power supply unit installed.
   - Predicting failure—Power supply is present but predicting failure.
   - FAULTY—Power supply is present but faulty (no power cable, power switch turned off, fuse blown, or other internal error).

To display temperature status:

1. Connect to the switch and log in as admin.
2. Enter the **tempShow** command:

```
switch:admin> tempshow
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Status</th>
<th>Centigrade</th>
<th>Fahrenheit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OK</td>
<td>21</td>
<td>70</td>
</tr>
<tr>
<td>2</td>
<td>OK</td>
<td>22</td>
<td>72</td>
</tr>
<tr>
<td>3</td>
<td>OK</td>
<td>29</td>
<td>84</td>
</tr>
<tr>
<td>4</td>
<td>OK</td>
<td>24</td>
<td>75</td>
</tr>
<tr>
<td>5</td>
<td>OK</td>
<td>25</td>
<td>77</td>
</tr>
</tbody>
</table>

```
switch:admin>
```

Information displays for each temperature sensor in the switch. The possible temperature status values are:

- **OK**—Temperature is within acceptable range.
- **FAIL**—Temperature is outside of acceptable range. Damage might occur.

### Viewing the system message log

The system message log feature enables messages to be saved across power cycles and reboots.

4/256 SAN Director and DC SAN Backbone Director (short name, DC Director) models maintain an independent system message log for each of the two CP blades. For these models, you should configure **syslogd** to support chronological system message logs. For details, see “Configuring for syslogd” on page 298.

For details on error messages, see the *Fabric OS Command Reference*. To display the system message log, with no page breaks:

1. Connect to the switch and log in as admin.
2. Enter the **errDump** command.

To display the system message log one at a time:

1. Connect to the switch and log in as admin.
2. Enter the **errShow** command.

To clear the system message log:

1. Connect to the switch and log in as admin.
2. Enter the **errClear** command.

All switch and chassis events are removed.

### Viewing the port log

The Fabric OS maintains an internal log of all port activity. The port log stores entries for each port as a circular buffer. Each port has space to store 8000 log entries. When the log is full, the newest log entries overwrite the oldest log entries. Port logs are not persistent and are lost over power-cycles and reboots. If the port log is disabled, an error message displays.

**NOTE:** Port log functionality is completely separate from the system message log. Port logs are typically used to troubleshoot device connections.

To view the port log:

1. Connect to the switch and log in as admin.
2. Enter the `portLogShow` command:

```
switch:admin> portlogshow 12
```

```
time          task       event  port  cmd  args
                        --------------------------------------------------
Thu Apr 14 12:07:09 2005
12:07:09.350  PORT       Rx       0   40
02fffffd,00fffffd,0608ffff,14000000
12:07:09.350  PORT       Tx       0    0  c0fffffd,00fffffd,060807fc
12:07:10.812  PORT       Tx       0   40
02fffffd,00fffffd,07feffff,14000000
12:07:10.813  PORT       Rx       0    0  c0fffffd,00fffffd,07fe0627
12:07:19.492  PORT       Tx       4   40
02fffffd,00fffffd,0800ffff,14000000
12:07:19.492  PORT       Tx      22   40
02fffffd,00fffffd,0802ffff,14000000
12:07:19.493  PORT       Rx      4    0  c0fffffd,00fffffd,08009287
12:07:19.493  PORT       Tx      24   40
02fffffd,00fffffd,0804ffff,14000000
12:07:19.494  PORT       Tx      31   40
02fffffd,00fffffd,0806ffff,14000000
12:07:19.494  PORT       Rx      22    0  c0fffffd,00fffffd,0802928d
12:07:19.494  PORT       Rx      24    0  c0fffffd,00fffffd,080492a3
12:07:19.495  PORT       Rx      31    0  c0fffffd,00fffffd,080692a7
```

Use the commands summarized in Table 65 to view and manage port logs. See the Fabric OS Command Reference for additional information about these commands.

**Table 65  Commands for port log management**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portLogClear</td>
<td>Clear port logs for all or particular ports.</td>
</tr>
<tr>
<td>portLogDisable</td>
<td>Disable port logs for all or particular ports.</td>
</tr>
<tr>
<td>portLogDump</td>
<td>Display port logs for all or particular ports, without page breaks.</td>
</tr>
<tr>
<td>portLogEnable</td>
<td>Enable port logs for all or particular ports.</td>
</tr>
<tr>
<td>portLogShow</td>
<td>Display port logs for all or particular ports, with page breaks.</td>
</tr>
</tbody>
</table>

The `portLogDump` command output (trace) is a powerful tool that is used to troubleshoot fabric issues. The `portLogDump` output provides detailed information about the actions and communications within a fabric. By understanding the processes that are taking place in the fabric, issues can be identified and located.

The `portLogDump` command displays the port log, showing a portion of the Fibre Channel payload and header (FC-PH). The header contains control and addressing information associated with the frame. The payload contains the information being transported by the frame and is determined by the higher-level service or FC_4 upper level protocol. There are many different payload formats based on the protocol.
Because a `portLogDump` output is long, a truncated example is presented:

```
switch:admin> portlogdump
task event port cmd args
--------------------------------------------------------------------------------
16:30:41.780 PORT Rx 9 40 02fffffd,00fffffd,0061ffff,14000000
16:30:41.780 PORT Tx 9 0 c0fffffd,00fffffd,0061030f
16:30:42.503 PORT Tx 9 40 02fffffd,00fffffd,0310ffff,14000000
16:30:42.505 PORT Rx 9 0 c0fffffd,00fffffd,03100062
16:31:00.464 PORT Rx 9 20 02fffc01,00ffca0,0063ffff,01000000
16:31:00.464 PORT Tx 9 0 c0fffc01,00ffca0,00630311
16:31:00.465 nsd ctin 9 fc 000104a0,0000007f
16:31:00.465 nsd ctout 9 fc 00038002,00000003,01fffc01
16:31:00.466 PORT Tx 9 0356 03fffc01,00000000,00000002
16:31:00.474 PORT Rx 9 0 c0fffc01,00ffca0,00630311
16:31:01.844 PORT Tx 9 40 02fffffd,00fffffd,0312ffff,14000000
16:31:01.854 PORT Rx 9 0 c0fffffd,00fffffd,03120064
16:31:01.963 PORT Rx 9 40 02fffffd,00fffffd,0065ffff,14000000
16:31:01.963 PORT Tx 9 0 c0fffffd,00fffffd,00650313
16:31:14.726 INTR pstate 0 LF2
16:31:14.729 PORT scn 0 137 00000000,00000000,00000008
16:31:14.729 PORT scn 0 129 00000000,00000000,00000000
16:31:14.729 PORT scn 0 2 00010004,00000000,00000000
16:31:14.730 SPEE sn 0 ws 00000002,00000000,00000000
```

<output truncated>

### Configuring for syslogd

The system logging daemon (**syslogd**) is a process on UNIX, Linux, and some Windows systems that reads and logs messages as specified by the system administrator.

Fabric OS can be configured to use a UNIX-style syslogd process to forward system events and error messages to log files on a remote host system. The host system can be running UNIX, Linux, or any other operating system that supports the standard syslogd functionality.

Fabric OS supports UNIX local7 facilities (the default facility level is 7). Configuring for syslogd involves configuring the host, enabling syslogd on the switch, and, optionally, setting the facility level.

### Configuring the host

Fabric OS supports a subset of UNIX-style message severities that default to the UNIX local7 facility. To configure the host, edit the `/etc/syslog.conf` file to map Fabric OS message severities to UNIX severities, as shown in Table 66.

**Table 66** Fabric OS to UNIX message severities

<table>
<thead>
<tr>
<th>Fabric OS message severity</th>
<th>UNIX message severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical (1)</td>
<td>Emergency (0)</td>
</tr>
<tr>
<td>Error (2)</td>
<td>Error (3)</td>
</tr>
<tr>
<td>Warning (3)</td>
<td>Warning (4)</td>
</tr>
<tr>
<td>Info (4)</td>
<td>Info (6)</td>
</tr>
</tbody>
</table>
In this example, Fabric OS messages map to local7 facility level 7 in the `/etc/syslog.conf` file:

```
local7.emerg  /var/adm/swcritical
local7.alert  /var/adm/alert7
local7.crit   /var/adm/crit7
local7.err    /var/adm/swerror
local7.warning /var/adm/swwarning
local7.notice  /var/adm/notice7
local7.info   /var/adm/swinfo
local7.debug  /var/adm/debug7
```

If you prefer to map Fabric OS severities to a different UNIX local7 facility level, see "To set the facility level:" on page 299.

**Configuring the switch**

Configuring the switch involves specifying syslogd hosts and, optionally, setting the facility level. You can also remove a host from the list of syslogd hosts.

To specify syslogd hosts:

1. Connect to the switch and log in as admin.
2. Enter the `syslogdipAdd` command and specify an IP address.
3. Verify that the IP address was entered correctly, using the `syslogdipShow` command.

   The `syslogdipadd` command accepts IPv4 and IPv6 addresses. You can specify up to six host IP addresses for storing syslog messages, as shown in this example:

   ```
   switch:admin> syslogdipadd 1080::8:800:200C:417A
   switch:admin> syslogdipadd 1081::8:800:200C:417A
   switch:admin> syslogdipadd 1082::8:800:200C:417A
   switch:admin> syslogdipadd 10.1.2.4
   switch:admin> syslogdipadd 10.1.2.5
   switch:admin> syslogdipadd 10.1.2.6
   ```

   To set the facility level:

   1. Connect to the switch and log in as admin.
   2. Enter the following command:

   ```
   switch:admin> syslogdfacility -l n
   ```

   `n` is a number from 0 through 7, indicating a UNIX local7 facility. The default is 7.

   It is necessary to set the facility level only if you specified a facility other than local7 in the host `/etc/syslog.conf` file.
To remove a syslogd host from the list:
1. Connect to the switch and log in as admin.
2. Enter the `syslog Dip Remove` command:
   
   ```
   switch:admin> syslog Dip Remove 10.1.2.1
   ```
3. Verify the IP address was deleted using the `syslog Dip Show` command.

**Viewing and saving diagnostic information**

Enter the `support Show` command to dump important diagnostic and status information to the session screen, where you can review it or capture its data.

To save a set of files that customer support technicians can use to further diagnose the switch condition, enter the `support Save` command. The command prompts for an FTP server, packages the following files, and sends them to the specified server:

- The output of the `support Show` command
- The contents of any trace dump files on the switch
- System message logs (for Directors, `support Save` saves the system message logs from both of the CP blades)

See “Setting up automatic trace dump transfers”, next.

**Setting up automatic trace dump transfers**

You can set up a switch so that diagnostic information is transferred automatically to a remote server. If a problem occurs, you can then provide your customer support representative with the most detailed information possible. To ensure the best service, you should set up for automatic transfer as part of standard switch configuration, before a problem occurs.

Setting up for automatic transfer of diagnostic files involves the following tasks:

- Specifying a remote server to store the files.
- Enabling the automatic transfer of trace dumps to the server. (Trace dumps overwrite each other by default; sending them to a server preserves information that would otherwise be lost.)
- Setting up a periodic checking of the remote server so that you are alerted if the server becomes unavailable and you can correct the problem.

After the setup is complete, you can run the `support Save` command to save RASLog, TRACE, supportShow, core file, FFDC data and other diagnostic support information to the server without specifying server details.

The following procedures describe the tasks for setting up automatic transfer. For details on the commands, see the Fabric OS Command Reference.

To specify a remote server:

1. Verify that the FTP service is running on the remote server.
2. Connect to the switch and log in as admin.
3. Enter the following command:
   
   ```
   switch:admin> support ftp -s
   ```
   The command is interactive.
4. Respond to the prompts as follows:

- **Host Name**: Enter the name or IP address of the server where the file is to be stored; for example, 1080::8:800:200C:417A for a server configured for IPv6.
- **User name**: Enter the user name of your account on the server; for example, “JohnDoe”.
- **Password**: Enter your account password for the server.
- **Remote directory**: Specify a path name for the remote directory. Absolute path names can be specified by starting the path name with a forward slash (/). Specifying a relative path name will create the directory in the user’s home directory on UNIX servers, and in the directory where the FTP server is running on Windows servers.

To enable the automatic transfer of trace dumps:

1. Connect to the switch and log in as admin.
2. Enter the following command:
   ```
   switch:admin> supportftp -e
   Support auto file transfer enabled.
   ```

To set up periodic checking of the remote server:

1. Connect to the switch and log in as admin.
2. Enter the following command:
   ```
   switch:admin> supportftp -t interval
   Specify the interval in hours, for example:
   switch:admin> supportftp -t 4
   supportftp: ftp check period changed
   ```
   The minimum interval is 1 hour. Specify 0 hours to disable the checking feature.

To save a comprehensive set of diagnostic files to the server:

1. Connect to the switch and log in as admin.
2. Enter the following command:
   ```
   switch:admin> supportsave -c
   The command is interactive.
   ```
3. Respond to the prompts as follows:
   - **User name**: Enter the user name of your account on the server; for example, “JohnDoe”.
   - **Password**: Enter your account password for the server.
   - **Remote directory**: Specify a path name for the remote directory. Absolute path names can be specified by starting the path name with a forward slash (/). Specifying a relative path name will create the directory in the user’s home directory on UNIX servers, and in the directory where the FTP server is running on Windows servers.
14 Troubleshooting

This chapter provides information on troubleshooting and the most common procedures to use to diagnose and recover from problems. It also includes specific troubleshooting scenarios as examples.

About troubleshooting

Troubleshooting should begin at the center of the SAN—the fabric. Because switches are located between the hosts and storage devices and have visibility into both sides of the storage network, starting with them can help narrow the search path. After eliminating the possibility of a fault within the fabric, see if the problem is on the storage side or the host side, and continue a more detailed diagnosis from there. Using this approach can quickly pinpoint and isolate problems.

For example, if a host cannot detect a storage device, run a switch command, for example `switchShow` to determine if the storage device is logically connected to the switch. If not, focus first on the switch directly connecting to storage. Use the diagnostic tools in Table 67 to better understand why it is not visible to the switch. If the storage can be detected by the switch, and the host still cannot detect the storage device, then there is still a problem between the host and switch.

Most common problem areas

Table 67 lists the most common problem areas that arise within SANs and identifies tools to use to resolve them.

Table 67 Common troubleshooting problems and tools

<table>
<thead>
<tr>
<th>Problem area</th>
<th>Investigate</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric</td>
<td>• Missing devices</td>
<td>• Switch LEDs</td>
</tr>
<tr>
<td></td>
<td>• Marginal links (unstable connections)</td>
<td>• Switch commands (for example, <code>switchShow</code> or <code>nsAllShow</code>) for diagnostics</td>
</tr>
<tr>
<td></td>
<td>• Incorrect zoning configurations</td>
<td>• Web or GUI-based monitoring and management software tools</td>
</tr>
<tr>
<td></td>
<td>• Incorrect switch configurations</td>
<td></td>
</tr>
<tr>
<td>Storage Devices</td>
<td>• Physical issues between switch and devices</td>
<td>• Device LEDs</td>
</tr>
<tr>
<td></td>
<td>• Incorrect storage software configurations</td>
<td>• Storage diagnostic tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Switch commands (for example, <code>switchShow</code> or <code>nsAllShow</code>) for diagnostics</td>
</tr>
</tbody>
</table>
Gathering information for technical support

If you are troubleshooting a production system, you must gather data quickly. As soon as a problem is observed, perform the following tasks (if using a dual CP system, run the commands on both CPs):

1. Enter the `supportSave` command to save RASLog, TRACE, and `supportShow` (active CP only) information for the local CP to a remote FTP location. On a dual CP system, only the local CP information is saved and `supportShow` information is only available on the active CP.

   **NOTE:** It is recommended that you use the `supportFtp` command to set up the `supportSave` environment for automatic dump transfers and the use of the `-n -c` options; this will save you from having to enter (or know) all the required FTP parameters needed to successfully execute a `supportSave` operation.

2. Enter the `pdShow` command to display data from a panic dump file. The panic dump file contains information that may be useful to determine the cause of the system panic.

3. Enter the `supportSave` command to save or remove core files created by daemons.

For more details about these commands, see the Fabric OS Command Reference.

Troubleshooting questions

Common steps and questions to ask when troubleshooting system problems:

1. What is the current Fabric OS level?
2. What is the switch hardware version?
3. Is the switch operational?
4. What and when were the last actions or changes made to the system environment?
5. Impact assessment and urgency:
   - Is the switch down?
   - Is it a standalone switch?
   - Are there VE, VEX or EX ports connected to the chassis?
• How large is the fabric?
• Is it a secure fabric?
• Is the fabric redundant?

6. Run the `supportSave` command on both CPs if it is a director class product, for example 4/256 SAN Director or DC SAN Backbone Director (short name, DC Director).

7. Document the sequence of events by answering the following questions:
   • What happened prior to the problem?
   • Is the problem reproducible?
   • If so, what are the steps to produce the problem?
   • What configuration was in place when the problem occurred?

8. Did a failover occur?
9. Was security enabled?
10. Was POST enabled?
11. Are serial port (console) logs available?
12. Which CP blade was active? (only applicable to the SAN Director 2/128, 4/256 SAN Director, and DC Director.

13. Obtain as much of the following informational items as possible prior to contacting HP technical support.
   • A description of the problem with the switch or the fault with the fabric.
   • Switch information:
     • Serial number (located on the chassis)
     • World Wide Name (obtain using `licenseIdShow` or `wwn` commands)
     • Fabric OS version (obtain using the `version` command)
   • The last actions or changes made to the system environment:
     • settings
     • `supportSave` output; you can save this information on a qualified and installed HP USB storage device only on the DC Director platform.
     • `pdShow` and `supportSave` output
   • Host information:
     • OS version and patch level
     • HBA type
     • HBA firmware version
     • HBA driver version
     • Configuration settings
   • Storage information:
     • Disk/tape type
     • Disk/tape firmware level
     • Controller type
     • Controller firmware level
     • Configuration settings
     • Storage software (such as EMC Control Center, Veritas SPC, etc.)
Analyzing connection problems

If a host is unable to detect its target (for example, a storage or tape device), you should begin troubleshooting the problem in the middle of the data path. Determine if the problem is above or below the starting point, then continue to divide the suspected problem path in half until you can pinpoint the problem.

To check the logical connection:

1. Enter the `switchShow` command.
2. Review the output and determine if the device successfully logged into the switch:
   - A device that is logically connected to the switch is registered as an F_Port or L_Port.
   - A device that is not logically connected to the switch will be registered as something other than an F_Port or L_Port, for example a G-Port.
3. If the missing device is logically connected, proceed to the next troubleshooting procedure “To check the name server (NS):” on page 308.
4. If the missing device is not logically connected, check the device and everything on that side of the data path. Also see “Correcting link failures” on page 319 for additional information.

   This includes all aspects of the host OS, the driver settings and binaries, the device Basic Input Output System (BIOS) settings, the SFP, the cable going from the switch to the device, the SFP on the switch side of that cable, and all switch settings related to the device. See “To check for a loop initialization failure.” on page 320 as the next potential trouble spot.

To check for Fibre Channel connectivity problems:

1. Enter the `fcPing` command, which:
   - Checks the zoning configuration for the two ports specified.
   - Generates an Extended Link Service frame (ELS) ECHO request to the source port specified and validates the response.
   - Generates an ELS ECHO request to the destination port specified and validates the response.

   Regardless of the device’s zoning, the `fcPing` command sends the ELS frame to the destination port. A device can take any of the following actions:
   - Send an ELS Accept to the ELS request.
   - Send an ELS Reject to the ELS request.
   - Ignore the ELS request.

   There are some devices that do not support the ELS ECHO request. In these cases, the device will either not respond to the request or send an ELS reject. When a device does not respond to the ELS request, further debugging is required; however, do not assume that the device is not connected to the Fibre Channel.

   Following is sample output from the `fcPing` command in which one device accepts the request and another device rejects the request:

   ```plaintext
   switch:admin> fcPing 10:00:00:00:c9:29:0e:c4 21:00:00:20:37:25:ad:05
   Source: 10:00:00:00:c9:29:0e:c4
   Destination: 21:00:00:20:37:25:ad:05
   Zone Check: Not Zoned
   Pinging 10:00:00:00:c9:29:0e:c4 [0x20800] with 12 bytes of date:
   received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1162 usec
   received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1013 usec
   received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1442 usec
   received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1052 usec
   received reply from 10:00:00:00:c9:29:0e:c4: 12 bytes time:1012 usec
   5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
   ```
Round-trip min/avg/max = 1012/1136/1442 usec

Pinging 21:00:00:20:37:25:ad:05 [0x211e8] with 12 bytes of data:
Request rejected
Request rejected
Request rejected
Request rejected
Request rejected
5 frames sent, 0 frames received, 5 frames rejected, 0 frames timeout
Round-trip min/avg/max = 0/0/0 usec

Following is sample output from the fcPing command in which one device accepts the request and another device does not respond to the request:

switch:admin> fcping 0x020800 22:00:00:04:cf:75:63:85
Source: 0x20800
Destination: 22:00:00:04:cf:75:63:85
Zone Check: Zoned

Pinging 0x020800 with 12 bytes of data:
received reply from 0x020800: 12 bytes time:1159 usec
received reply from 0x020800: 12 bytes time:1006 usec
received reply from 0x020800: 12 bytes time:1008 usec
received reply from 0x020800: 12 bytes time:1038 usec
received reply from 0x020800: 12 bytes time:1010 usec
5 frames sent, 5 frames received, 0 frames rejected, 0 frames timeout
Round-trip min/avg/max = 1006/1044/1159 usec

Pinging 22:00:00:04:cf:75:63:85 [0x217d9] with 12 bytes of data:
Request timed out
Request timed out
Request timed out
Request timed out
Request timed out
5 frames sent, 0 frames received, 0 frames rejected, 5 frames timeout
Round-trip min/avg/max = 0/0/0 usec

For details about the fcPing command, see the Fabric OS Command Reference.
To check the name server (NS):

1. Enter the `nsShow` command on the switch to which the device is attached:

   The Local Name Server has 9 entries:

<table>
<thead>
<tr>
<th>Type</th>
<th>Pid</th>
<th>COS</th>
<th>PortName</th>
<th>NodeName</th>
<th>TTL (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>*N</td>
<td>021a00;</td>
<td>2,3</td>
<td>20:00:00:e0:69:f0:07:c6;10:00:00:e0:69:f0:07:c6;</td>
<td>895</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Port Name: 20:0a:00:60:69:10:8d:fd</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>051edc;</td>
<td>3,21</td>
<td>20:37:d9:77:96;20:00:00:20:37:d9:77:96; na</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Port Name: 20:0e:00:60:69:10:9b:5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>051ee0;</td>
<td>3,21</td>
<td>20:37:d9:73:0f;20:00:00:20:37:d9:73:0f; na</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Port Name: 20:0e:00:60:69:10:9b:5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>051ee1;</td>
<td>3,21</td>
<td>20:37:d9:76:0f;20:00:00:20:37:d9:76:0f; na</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Port Name: 20:0e:00:60:69:10:9b:5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>051ee2;</td>
<td>3,21</td>
<td>20:37:d9:77:5a;20:00:00:20:37:d9:77:5a; na</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Port Name: 20:0e:00:60:69:10:9b:5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>051ee4;</td>
<td>3,21</td>
<td>20:37:d9:74:0f;20:00:00:20:37:d9:74:0f; na</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Port Name: 20:0e:00:60:69:10:9b:5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>051ee8;</td>
<td>3,21</td>
<td>20:37:d9:6f:eb;20:00:00:20:37:d9:6f:eb; na</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Port Name: 20:0e:00:60:69:10:9b:5b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL</td>
<td>051ee8;</td>
<td>3,21</td>
<td>20:37:d9:6f:eb;20:00:00:20:37:d9:6f:eb; na</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Port Name: 20:0e:00:60:69:10:9b:5b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Look for the device in the NS list, which lists the nodes connected to that switch. This allows you to determine if a particular node is accessible on the network.

   - If the device is not present in the NS list, the problem is between the device and the switch. There may be a time-out communication problem between edge devices and the name server, or there may be a login issue. First check the edge device documentation to determine if there is a time-out setting or parameter that can be reconfigured. Also, check the port log for NS registration information and FCP probing failures (using the `fcpProbeShow` command). If these queries do not help solve the problem, contact the support organization for the product that appears to be inaccessible.
• If the device is listed in the NS, the problem is between the storage device and the host. There may be a zoning mismatch or a host/storage issue. Proceed to “To check for zoning problems:” on page 309.

3. Enter the portLoginShow command to check the port login status.

4. Enter the fcpProbeShow command to display the FCP probing information for the devices attached to the specified F_Port or L_Port. This information includes the number of successful logins and SCSI INQUIRY commands sent over this port and a list of the attached devices.

5. Check the port log to determine whether or not the device sent the FLOGI frame to the switch, and the switch probed the device.

To check for zoning problems:

1. Enter the cfgActvShow command to determine if zoning is enabled.
   If zoning is enabled, it is possible that the problem is being caused by zoning enforcement (for example, two devices in different zones cannot detect each other).
   If zoning is disabled, check the default zone mode by entering the defzone --show command. If it is no access, change it to all access. To modify default zone mode from no access to all access, enter the defzone --all command, and then the cfgsave command.

2. Confirm that the specific edge devices that must communicate with each other are in the same zone.
   • If they are not in the same zone and zoning is enabled, proceed to step 3.
   • If they are in the same zone, perform the following tasks:
      • Enter the portCamShow command on the host port to verify that the target is present.
      • Enter the portCamShow command on the target.
      • Enter the nsZoneMember command with the port ID for the zoned devices on the host and target to determine whether the name server is aware that these devices are zoned together.

3. Resolve zoning conflicts by putting the devices into the same zoning configuration.

4. Enter the defzone --show command to display the current state of the zone access mode and the access level. The defzone command sets the default zone access mode to No Access.

```
switch:admin> defzone --show
Default Zone Access Mode
committed - No Access
transaction - No Transaction
```

See “Correcting zoning setup issues” on page 311 for additional information.

---

Restoring a segmented fabric

Fabric segmentation is generally caused by:

• Incompatible fabric parameters (see “To reconcile fabric parameters individually:” on page 310).
• Incorrect PID setting (see “Configuring the PID Format” on page 489).
• Incompatible zoning configuration.

If fabric segmentation is caused by “zone conflict”, verify following:

• The activate cfg (zone set) on each end of segmented ISL must be same.
• Any zone object with the same name must have same the type and contents.

If fabric segmentation is caused by and “incompatible zone database”, check following:

• Whether the merge results in an over limit zone database? Different FOS versions support different zone database sizes, for example pre FOS-v5.2 supports 256Kbytes and FOSv5.2 and later support 1Mbytes.
• Whether any port number greater than 255 is configured in a port zone? Any pre FOS-v5.2 switch will not merge with a newer switches with a port index greater than 255.
• Domain ID conflict (see “To reconcile a domain ID conflict:” on page 310).
• A switch in a secure fabric not running Secure Fabric OS.

See the Secure Fabric OS Administrator’s Guide for additional information.
There are a number of settings that control the overall behavior and operation of the fabric. Some of these values, such as the Domain ID, are assigned automatically by the fabric and can differ from one switch to another in the fabric. Other parameters, such as the BB credit, can be changed for specific applications or operating environments, but must be the same among all switches to allow the formation of a fabric.

The following fabric parameters must be identical for a fabric to merge:

- R_A_TOV
- E_D_TOV
- Data field size
- Sequence level switching
- Disable device probing
- Suppress class F traffic
- Per-frame route priority
- Long distance fabric (not necessary on Bloom-based, Condor, or GoldenEye fabrics)
- BB credit
- PID format

To reconcile fabric parameters individually:

1. Log in to one of the segmented switches as admin.
2. Enter the `configShow` command.
3. Log in to another switch in the same fabric as admin.
4. Enter the `configShow` command.
5. Compare the two switch configurations line by line and look for differences. Do this by comparing the two Telnet windows or by printing the `configShow` output. Also, verify that the fabric parameter settings (see the above list) are the same for both switches.
6. Connect to the segmented switch after the discrepancy is identified.
7. Disable the switch by entering the `switchDisable` command.
8. Enter the `configure` command to edit the fabric parameters for the segmented switch.
   See the Fabric OS Command Reference for more detailed information.
9. Enable the switch by entering the `switchEnable` command.

Alternatively, you can reconcile fabric parameters by entering the `configUpload` command for each switch.

To download a correct configuration:

You can restore a segmented fabric by downloading a previously saved correct backup configuration to the switch. Downloading in this manner reconciles any discrepancy in the fabric parameters and allows the segmented switch to rejoin the main fabric. For details on uploading and downloading configurations, see “Maintaining Configurations” on page 131.

To reconcile a Domain ID conflict:

If a Domain ID conflict appears, the conflict is only reported at the point where the two fabrics are physically connected. However, there may be several conflicting Domain IDs, which appears as soon as the initial conflict is resolved.

Typically, the fabric automatically resolves domain conflicts during fabric merges or builds unless Insistent Domain ID (IDID) is configured. If IDID is enabled, switches that cannot be programmed with a unique Domain ID are segmented out. Check each switch that has IDID configured and make sure their Domain IDs are unique within the configuration.

Repeat this procedure until all Domain ID conflicts are resolved:

1. Enter the `fabricShow` command on a switch from one of the fabrics.
2. In a separate Telnet window, enter the `fabricShow` command on a switch from the second fabric.
3. Compare the `fabricShow` output from the two fabrics. Note the number of Domain ID conflicts; there may be several duplicate Domain IDs that must be changed. Determine which switches have domain overlap and change the Domain IDs for each of those switches.

4. Choose the fabric on which to change the duplicate Domain ID; connect to the conflicting switch in that fabric.

5. Enter the `switchDisable` command.

6. Enter the `switchEnable` command.

   This will enable the joining switch to obtain a new Domain ID as part of the process of coming online. The fabric principal switch will allocate the next available Domain ID to the new switch during this process.

7. Repeat step 4 through step 6 if additional switches have conflicting Domain IDs.

### Correcting zoning setup issues

Table 68 lists the types of zone configuration discrepancies that can cause segmentation.

<table>
<thead>
<tr>
<th>Conflict cause</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration mismatch</td>
<td>Occurs when zoning is enabled in both fabrics and the zone configurations that are enabled are different in each fabric.</td>
</tr>
<tr>
<td>Type mismatch</td>
<td>Occurs when the name of a zone object in one fabric is also used for a different type of zone object in the other fabric. A zone object is any device in a zone.</td>
</tr>
<tr>
<td>Content mismatch</td>
<td>Occurs when the definition in one fabric is different from the definition of a zone object with the same name in the other fabric.</td>
</tr>
</tbody>
</table>

Table 69 summarizes commands that are useful for debugging zoning issues.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>aliCreate</td>
<td>Use to create a zone alias.</td>
</tr>
<tr>
<td>aliDelete</td>
<td>Use to delete a zone alias.</td>
</tr>
<tr>
<td>cfgCreate</td>
<td>Use to create a zone configuration.</td>
</tr>
<tr>
<td>cfgShow</td>
<td>Displays zoning configuration.</td>
</tr>
<tr>
<td>cfgTransAbort</td>
<td>Use to abort the current zoning transaction without committing it.</td>
</tr>
<tr>
<td>cfgTransShow</td>
<td>Use to display the ID of the current zoning transaction.</td>
</tr>
<tr>
<td>defZone</td>
<td>Sets the default zone access mode to <code>No Access</code>, initializes a zoning transaction (if one is not already in progress), and creates the reserved zoning objects.</td>
</tr>
<tr>
<td>licenseShow</td>
<td>Displays current license keys and associated (licensed) products.</td>
</tr>
<tr>
<td>switchShow</td>
<td>Displays currently enabled configuration and any E_Port segmentations due to zone conflicts.</td>
</tr>
<tr>
<td>zoneAdd</td>
<td>Use to add a member to an existing zone.</td>
</tr>
<tr>
<td>zoneCreate</td>
<td>Use to create a zone. Before a zone becomes active, the <code>cfgSave</code> and <code>cfgEnable</code> commands must be used.</td>
</tr>
<tr>
<td>zoneHelp</td>
<td>Displays help information for zone commands.</td>
</tr>
<tr>
<td>zoneShow</td>
<td>Displays zone information.</td>
</tr>
</tbody>
</table>
See “Administering Advanced Zoning” on page 403 for additional information about setting up zoning. Also, see the Fabric OS Command Reference for details about zoning commands.

You can correct zone conflicts by using the cfgClear command to clear the zoning database.

**IMPORTANT:** The cfgClear command is a disruptive procedure.

To correct a fabric merge problem quickly:

1. Determine which switch(es) have the incorrect zoning configuration; then, log in to the switches as admin.
2. Enter the switchDisable command.
3. Enter the cfgDisable command.
4. Enter the cfgClear command.
   - The cfgClear command clears the zoning database on the affected switches.
5. Enter the switchEnable command. This forces a zone merge and populates the switches with the desired zoning database. The two fabrics will be merged again.

To correct a merge conflict without disrupting the fabric, first verify a fabric merge problem, then edit zone configuration members, and then reorder the zone member list.

To verify a fabric merge problem:

1. Enter the switchShow command to validate that the segmentation is due to a zone issue.
2. See Table 68 to view the different types of zone discrepancies and determine what might be causing the conflict.

To edit zone configuration members:

1. Log in to one of the switches in a segmented fabric as admin.
2. Enter the cfgShow command and print the output.
3. Start another Telnet session and connect to the next fabric as an administrator.
4. Enter the cfgShow command and print the output.
5. Compare the two fabric zone configurations line by line and look for an incompatible configuration.
6. Connect to one of the fabrics.
7. Run zone configure edit commands to edit the fabric zone configuration for the segmented switch (see Table 69 on page 311 for specific commands).
   - If the zoneset members between two switches are not listed in the same order in both configurations, the configurations are considered a mismatch; this results in the switches being segmented in the fabric.
   - For example:
     ```
     [cfg1 = z1; z2]
     ```
     is different from
     ```
     [cfg1 = z2; z1]
     ```
     even though the members of the configuration are the same.
     - One simple approach to making sure that the zoneset members are in the same order is to keep the members in alphabetical order.

To reorder the zone member list:

1. Obtain the output from the cfgShow for both switches.
2. Compare the order in which the zone members are listed. Members must be listed in the same order.
3. Rearrange zone members so the configuration for both switches is the same. Arrange zone members in alphabetical order, if possible.
Recognizing MQ-WRITE errors

An MQ error is a message queue error. Identify an MQ error message by looking for the two letters M and Q in the error message:

```
2004/08/24-10:04:42, [MQ-1004], 218,, ERROR, ras007, mqRead, queue = raslog-test-string0123456-raslog, queue l
D = 1, type = 2
```

MQ errors can result in devices dropping from the SNS or can prevent a switch from joining the fabric. MQ errors are rare and difficult to troubleshoot; resolve them by working with HP. When encountering an MQ error, issue the `supportSave` command to capture debug information about the switch; then, forward the `supportSave` data to the switch supplier for further investigation.
Correcting I²C bus errors

I²C bus errors generally indicate defective hardware or poorly seated devices or blades; the specific item is listed in the error message. See the Fabric OS Command Reference for information specific to the error that was received. Some Chip-Port (CPT) and Environmental Monitor (EM) messages contain I²C-related information.

If the I²C message does not indicate the specific hardware that may be failing, begin debugging the hardware, as this is the most likely cause. The next sections provide procedures for debugging the hardware.

To check fan components:

1. Log in to the switch as user.
2. Enter the `fanShow` command.
3. Check the fan status and speed output.

If any of the fan speeds display abnormal RPMs, replace the fan. You may first consider re-seating the fan (unplug it and plug it back in).

To check the switch temperature:

1. Log in to the switch as user.
2. Enter the `tempShow` command.
3. Check the temperature output.

Look for indications of high or low temperatures.

To check the power supply:

1. Log in to the switch as user.
2. Enter the `psShow` command.
3. Check the power supply status. Refer to the appropriate hardware reference manual for details regarding the power supply status.
   
   If any of the power supplies show a status other than OK, consider replacing the power supply as soon as possible.

To check the temperature, fan, and power supply:

1. Log in to the switch as user.
2. Enter the `sensorShow` command. See the Fabric OS Command Reference for details regarding the sensor numbers.
3. Check the temperature output.
   
   Look for indications of high or low temperatures.
4. Check the fan speed output.
   
   If any of the fan speeds display abnormal RPMs, replace the fan FRU.
5. Check the power supply status.
   
   If any power supplies show a status other than OK, consider replacing the power supply as soon as possible.
Correcting device login issues

Perform the following steps to try to pinpoint problems with device logins.

1. Log in to the switch as admin.
2. Enter the `switchShow` command; then, check for correct logins:

```
switch:admin> switchshow
switchName:     Dazzler
switchType:     26.1
switchState:    Online
switchMode:     Native
switchRole:     Principal
switchDomain:   1
switchId:       fffc01
switchWwn:      10:00:00:05:1e:34:00:70
zoning:         OFF
switchBeacon:   OFF

Area Port Media Speed State     Proto
=====================================  
   0   0   id    AN   Port_Flt                 
   1   1   id    N2   Online           F-Port  21:00:00:e0:8b:13:08:10 
   2   2   id    N2   No_Light            
   3   3   --    N2   No_Module            
   4   4   --    N2   No_Module            
   5   5   id    N2   No_Light            
   6   6   --    N2   No_Module            
   7   7   --    N2   No_Module            
   8   8   id    N2   No_Light            
   9   9   id    N2   No_Light            
  10  10   --    N2   No_Module            
  11  11   --    N2   No_Module            
  12  12   --    N2   No_Module            
  13  13   --    N2   No_Module            
  14  14   id    N2   Online           F-Port  21:00:00:e0:8b:12:8a:be 
  15  15   id    N2   Online           E-Port  segmented, (No Fabric License)
```

3. Enter the `portCfgShow` command to see if the port is configured correctly:

```
switch:admin> portcfgshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
```

switch:admin>

4. Enter the `portFshow` command to see if the port is configured correctly:

```
switch:admin> portfshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
```

switch:admin>

5. Enter the `portEnable` command to enable the port:

```
switch:admin> portenable
```

6. Enter the `portDisable` command to disable the port:

```
switch:admin> portdisable
```

7. Enter the `portCfgShow` command to see if the port is configured correctly:

```
switch:admin> portcfgshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
```

switch:admin>

8. Enter the `portFshow` command to see if the port is configured correctly:

```
switch:admin> portfshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
```

switch:admin>

9. Enter the `portEnable` command to enable the port:

```
switch:admin> portenable
```

10. Enter the `portDisable` command to disable the port:

```
switch:admin> portdisable
```

11. Enter the `portCfgShow` command to see if the port is configured correctly:

```
switch:admin> portcfgshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
```

switch:admin>

12. Enter the `portFshow` command to see if the port is configured correctly:

```
switch:admin> portfshow
Ports of Slot 0    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
```

switch:admin>
Enter the `portErrShow` command; then, check for errors that can cause login problems:
```
switch:admin> porterrshow
```
```
frames  enc  crc  too too  bad  enc disc link loss loss frjt fbsy
         tx   rx   in  err shrt long  eof  out  c3 fail sync  sig
===================================================================== 
0:   12m   0    0    0    0    0  3.8g   0    3    0    0    0    0
1:   17   18    0    0    0    0  1.4k   0    2    0    0    0    0
2:    0    0    0    0    0    0    0    0    2    0    0    0    0
3:    0    0    0    0    0    0    0    0    2    0    0    0    0
4:    0    0    0    0    0    0    0    3    0    0    0    0    0
5:    0    0    0    0    0    0    2    0    0    0    0    0    0
6:    0    0    0    0    0    0    2    0    0    0    0    0    0
7:    0    0    0    0    0    0    2    0    0    0    0    0    0
8:    0    0    0    0    0    0    3    0    0    0    0    0    0
9:    0    0    0    0    0    0    2    0    0    0    0    0    0
10:    0    0    0    0    0    0    2    0    0    0    0    0    0
11:    0    0    0    0    0    0    2    0    0    0    0    0    0
12:    0    0    0    0    0    0    3    0    0    0    0    0    0
13:    0    0    0    0    0    0    2    0    0    0    0    0    0
14:   17   18    0    0    0    0  222k   0    2    0    0    0    0
15:    6   22    0    0    0    0  150    0    2    0    0    0    0
```

- A high number of errors relative to the frames transmitted and frames received can indicate a marginal link (see “Correcting marginal links” on page 321 for additional information).
- A steadily increasing number of errors can indicate a problem. Track errors by sampling the port errors every five or ten minutes.

Enter the `portFlagsShow` command; then, check to see how a port has logged in and where a login failed (if a failure occurred):
```
switch:admin> portflagsshow
```
```
Port SNMP  Physical   Flags
-------------------------------
0 Offline   In_Sync    PRESENT U_PORT LED
1 Online    In_Sync    PRESENT ACTIVE F_PORT G_PORT U_PORT
LOGICAL_ONLINE LOGIN NOELP LED ACCEPT
2 Offline   No_Light   PRESENT U_PORT LED
3 Offline   No_Module  PRESENT U_PORT LED
4 Offline   No_Module  PRESENT U_PORT LED
5 Offline   No_Light   PRESENT U_PORT LED
6 Offline   No_Module  PRESENT U_PORT LED
7 Offline   No_Module  PRESENT U_PORT LED
```
8 Offline  No_Light  PRESENT U_PORT LED
9 Offline  No_Light  PRESENT U_PORT LED
10 Offline No_Module  PRESENT U_PORT LED
11 Offline No_Module  PRESENT U_PORT LED
12 Offline No_Module  PRESENT U_PORT LED
13 Offline No_Module  PRESENT U_PORT LED
14 Online  In_Sync  PRESENT ACTIVE F_PORT G_PORT U_PORT
LOGICAL_ONLINE LOGIN NOELP LED ACCEPT
15 Online  In_Sync  PRESENT ACTIVE E_PORT G_PORT U_PORT SEGMENTED
LOGICAL_ONLINE LOGIN LED

6. Enter the `portLogDumpPort portid` command where the port ID is the port number; then, view the device to switch communication.

```
switch:admin> portlogdump 13
time          task       event  port cmd  args
-------------------------------------------------
19:45:58.728  PORT       Tx3      0   12
22000000,00000000,ffffffff,11010000
19:45:58.778  SPEE       sn       0   WS  000000f0,00000000,00000000
19:45:58.787  SPEE       sn       0   WS  00000001,00000000,00000000
19:45:59.327  SPEE       sn       0   NC  00000002,00000000,00000000
19:45:59.328  LOOP       loopscn  0  LIP  8002
19:45:59.328  LOOP       loopscn  0  LIP  f7f7
19:45:59.328  PORT       Tx3      0   12
22000000,00000000,ffffffff,11010000
19:45:59.378  SPEE       sn       0   WS  000000f0,00000000,00000000
19:45:59.387  SPEE       sn       0   WS  00000001,00000000,00000000
19:45:59.927  SPEE       sn       0   NC  00000002,00000000,00000000
19:45:59.927  LOOP       loopscn  0  LIP  8002
19:45:59.928  LOOP       loopscn  0  LIP  f7f7
19:45:59.928  PORT       Tx3      0   12
22000000,00000000,ffffffff,11010000
```

**NOTE:** See “Viewing the port log” on page 306 for overview information about `portLogDump`.

### Identifying media-related issues

This section provides procedures that help pinpoint any media-related issues in the fabric. The tests listed in Table 70 are a combination of **structural** and **functional** tests that can be used to provide an overview of the hardware components and help identify media-related issues.

- **Structural** tests perform basic testing of the switch circuit. If a structural test fails, replace the main board or port blade.
- **Functional** tests verify the intended operational behavior of the switch by running frames through ports or bypass circuitry.
The following procedures are for checking switch-specific components.

To test a port’s external transmit and receive path:
1. Connect to the switch and log in as admin.
2. Connect the port you want to test to any other switch port with the cable you want to test.
3. Enter the `portloopbacktest -lb_mode 2` command.

To test a switch’s internal components:
1. Connect to the switch and log in as admin.
2. Connect the port you want to test to any other switch port with the cable you want to test.
3. Enter the `portloopbacktest -lb_mode 5` command where 5 is the operand that causes the test to run on the internal switch components (this is a partial list—see the Fabric OS Command Reference for additional command information):
   - `-nl_frames count`—Specify the number of frames to send.
   - `-lb_mode mode`—Select the loopback point for the test.
   - `-spd_mode mode`—Select the speed mode for the test.
   - `-ports itemlist`—Specify a list of user ports to test.

To test components to and from the HBA:
1. Connect to the switch and log in as admin.
2. Enter the `fPortTest` command as shown in this example (see the Fabric OS Command Reference for information on the command options).
   ```
   switchname:admin> fporttest 100,8,0xaa55,2, 512
   Will use pattern: aa55 aa55 aa55 aa55 aa55 aa55 ...
   Running fPortTest ........
   port 8 test passed.
   value = 0
   ```
   This example executed the `fPortTest` command 100 times on port 8 with payload pattern 0xaa55, pattern width 2 (meaning word width) and a default payload size of 512 bytes.

<table>
<thead>
<tr>
<th>Test name</th>
<th>Operands</th>
<th>Checks</th>
</tr>
</thead>
<tbody>
<tr>
<td>fporttest</td>
<td><code>[nl_frames count] [ports itemlist] [seed payload_pattern]</code></td>
<td>Tests point-to-point path from the F_Port to the N_Port and back. Used to test online F_Port devices, N_Port devices, SFPs, and GBICs.</td>
</tr>
<tr>
<td>loopporttest</td>
<td><code>[nl_frames count] [ports itemlist] [seed payload_pattern]</code></td>
<td>Only tests components attached to a switch that are on an FC-AL.</td>
</tr>
<tr>
<td>spinfab</td>
<td><code>[nmegs count] [ports itemlist] [setfail mode]</code></td>
<td>Tests switch-to-switch ISL cabling and trunk group operations.</td>
</tr>
</tbody>
</table>
Correcting link failures

A link failure occurs when a server or storage device is connected to a switch, but the link between the server/storage and the switch does not come up. This prevents the server/storage from communicating through the switch.

If the `switchShow` command or LEDs indicate that the link has not come up properly, use one or more of the following procedures.

The port negotiates the link speed with the opposite side. The negotiation usually completes in one or two seconds; however, sometimes the speed negotiation fails.

**NOTE:** Skip this procedure if the port speed is set to a static speed through the `portCfgSpeed` command.

To determine if the negotiation was successfully completed:

1. Enter the `portCfgShow` command to display the port speed settings of all the ports.
2. Enter the `switchShow` command to determine if the port has module light.
3. Determine whether or not the port at 1 Gbps completes by entering the `portCfgSpeed` command. Then change the port speed to 2 Gbps. This should correct the negotiation by setting to one speed.
4. Enter the `portLogShow` or `portLogDump` command.
5. Check the events area of the output:

   14:38:51.976  SPEE sn <Port#>   NC  00000001,00000000,00000001
   14:39:39.227  SPEE       sn      <Port#>   NC  00000002,00000000,00000001

   • `sn` indicates a speed negotiation.
   • `NC` indicates negotiation complete.

   If these fields do not appear, proceed to the step 6.

---

See Table 71 for a list of additional tests that can be used to determine the switch components that are not functioning properly. See the Fabric OS Command Reference for additional command information.

**Table 71  Switch component tests**

<table>
<thead>
<tr>
<th>Test</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>portloopbacktest</td>
<td>Performs a functional test of port N to N path.</td>
</tr>
<tr>
<td>portregtest</td>
<td>Performs a read and write test of the ASIC SRAMs and registers.</td>
</tr>
<tr>
<td>spinsilk</td>
<td>Performs a functional test of internal and external transmit and receive paths at full speed.</td>
</tr>
<tr>
<td>sramretentiontest</td>
<td>Verifies that the data written into the miscellaneous SRAMs in the ASIC are retained after a 10-second wait.</td>
</tr>
<tr>
<td>portloopbacktest</td>
<td>Verifies the functional components of the switch.</td>
</tr>
<tr>
<td>turboramtest</td>
<td>Verifies that the on chip SRAM located in the 2 Gbps ASIC is using the Turbo-Ram BIST circuitry. These same SRAMs are tested by <code>portregtest</code> and <code>sramretentiontest</code> using PCI operations, but for this test the BIST controller is able to perform the SRAM write and read operations at a much faster rate.</td>
</tr>
<tr>
<td>statstest</td>
<td>Verifies the ASIC statistics counter logic.</td>
</tr>
</tbody>
</table>

**Related Switch Test Option:**

| itemlist              | Restricts the items to be tested to a smaller set of parameter values that you pass to the switch. |
6. Correct the negotiation by entering the `portCfgSpeed [slotnumber/]portnumber, speed_level` command if the fields in step 5 do not appear.

```
switch:admin> portcfgspeed
```

Usage: `portCfgSpeed PortNumber Speed_Level`

- **Speed_Level**: 0 - Auto Negotiate
  - 1 - 1Gbps
  - 2 - 2Gbps
  - 4 - 4Gbps

To check for a loop initialization failure:

1. Verify the port is an L_Port.
   a. Enter the `switchShow` command.
   b. Check the comment field of the output to verify that the switch port indicates an L_Port. If a loop device is connected to the switch, the switch port must be initialized as an L_Port.
   c. Check to ensure that the port state is online; otherwise, check for link failures.

2. Verify the loop initialization if the port is not an L_Port.
   a. Enter the `portLogShow` or `portLogDump` command.
   b. Check argument number four for the **LISA frame** (0x11050100).

```
switch:admin> portlogdumpport 4
```

```
time          task       event  port cmd  args
--------------------------------------------------
11:40:02.078  PORT       Rx3     23   20
22000000,00000000,ffffffff,11050100 Received LISA frame
```

The **LISA frame** indicates that the loop initialization is complete.

3. Skip point-to-point initialization by using the `portCfgLport` command.

   The switch changes to point-to-point initialization after the Loop Initialization Soft Assigned (LISA) phase of the loop initialization. This behavior sometimes causes trouble with old HBAs.

To check for a point-to-point initialization failure:

1. Enter the `switchShow` command to confirm that the port is active and has a module that is synchronized.
   If a fabric device or another switch is connected to the switch, the switch port must be online.

2. Enter the `portLogShow` or `portLogDump` commands.

3. Verify the event area for the port state entry is `pstate`. The command entry `AC` indicates that the port has completed point-to-point initialization.

```
switch:admin> portlogdumpport 4
```

```
time          task       event  port cmd  args
--------------------------------------------------
11:38:21.726  INTR       pstate   4   AC
```

4. Skip over the loop initialization phase.

   After becoming an active port, the port becomes an F_Port or an E_Port depending on the device on the opposite side. If the opposite device is a fabric device, the port becomes an F_Port. If the opposite device is another switch, the port becomes an E_Port.

   If there is a problem with the fabric device, enter the `portCfgGPort` to force the port to try to come up as point-to-point only.

To correct a port that has come up in the wrong mode:

1. Enter the `switchShow` command.

2. Check the output from the `switchShow` command (see Table 72) and follow the suggested actions.
Correcting marginal links

A marginal link involves the connection between the switch and the edge device. Isolating the exact cause of a marginal link involves analyzing and testing many of the components that make up the link (including the switch port, switch SFP, cable, edge device, and edge device SFP).

To troubleshoot a marginal link:

1. Enter the `portErrShow` command.
2. Determine whether there is a relatively high number of errors (such as CRC errors or ENC_OUT errors), or if there are a steadily increasing number of errors to confirm a marginal link.
3. If you suspect a marginal link, isolate the areas by moving the suspected marginal port cable to a different port on the switch. Reseating of SFPs may also cure marginal port problems.
   - If the problem stops or goes away, the switch port or the SFP is marginal (proceed to step 4).
   - If the problem does not stop or go away, see step 7.
4. Replace the SFP on the marginal port.
5. Run the `portLoopbackTest` on the marginal port. You will need an adapter to run the loopback test for the SFP. Otherwise, run the test on the marginal port using the loopback mode `lb=5`. See the Fabric OS Command Reference for additional information on this command.

<table>
<thead>
<tr>
<th>Loopback mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Port Loopback (loopback plugs)</td>
</tr>
<tr>
<td>2</td>
<td>External (SERDES) loopback</td>
</tr>
<tr>
<td>5</td>
<td>Internal (parallel) loopback (indicates no external equipment)</td>
</tr>
<tr>
<td>7</td>
<td>Back-end bypass &amp; port loopback</td>
</tr>
</tbody>
</table>
6. Check the results of the loopback test and proceed as follows:
   - If the loopback test failed, the port is bad. Replace the port blade.
   - If the loopback test did not fail, the SFP was bad.

7. Optionally, to rule out cabling issues:
   a. Insert a new cable in the suspected marginal port.
   b. Enter the `portErrShow` command to determine if a problem still exists.
      - If the `portErrShow` output displays a normal number of generated errors, the issue is solved.
      - If the `portErrShow` output still displays a high number of generated errors, follow the troubleshooting procedures for the Host or Storage device.

### Inaccurate information in the system message log

In rare instances, events gathered by the track change feature can report inaccurate information to the system message log.

For example, a user enters a correct user name and password, but the login was rejected because the maximum number of users had been reached. However, when looking at the system message log, the login was reported as successful.

If the maximum number of switch users has been reached, the switch will still perform correctly in that it will reject the login of additional users (even if they enter correct user name and password information).

However, in this limited example, the Track Change feature will report this event inaccurately to the system message log; it will appear that the login was successful. This scenario only occurs when the maximum number of users has been reached; otherwise, the login information displayed in the system message log should reflect reality.

See “Tracking and controlling switch changes” on page 28 for information regarding enabling and disabling track changes (TC).

### Tracing Fibre Channel information

Frame Trace or FTRACE records user-defined messages and events on the Brocade FR4-18i and the 7500. The `portconfig` command uses the `ftrace` option to capture trace information on a per FCIP tunnel basis. You can configure up to eight FCIP tunnels on a single physical GE port. FTRACE is subject to the same FCIP tunnel limitations, such as tunnel disruption, port of switch disable or enable, and reboot requirements.

Tracing every FICON event affects performance. To avoid this, the default trace mask is set to 0x80000C7b. For troubleshooting, you should set the trace mask to 0-0xFFFFFFFF. The following table describes the configurable FTRACE parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Range</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto check Out</td>
<td>False</td>
<td>T/F</td>
<td>Boolean</td>
</tr>
<tr>
<td>Buffers</td>
<td>0</td>
<td>0-8</td>
<td>Integer</td>
</tr>
<tr>
<td>Display Mask</td>
<td>0xFFFF FFFF</td>
<td>0-0xFFFFFFFF</td>
<td>Integer</td>
</tr>
<tr>
<td>Enable</td>
<td>False</td>
<td>T/F</td>
<td>Boolean</td>
</tr>
<tr>
<td>Post Percentage</td>
<td>5</td>
<td>0-100</td>
<td>Integer</td>
</tr>
</tbody>
</table>

---

Table 73  Loopback modes

<table>
<thead>
<tr>
<th>Loopback mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Back-end bypass &amp; SERDES loopback</td>
</tr>
<tr>
<td>9</td>
<td>Back-end bypass &amp; internal loopback</td>
</tr>
</tbody>
</table>
After information is captured, you can use the `portshow` command to display FTRACE information on a GE port for a tunnel. You can save trace events can for future analysis.

### Configuring ftrace for a tunnel

Use the following syntax to configure a trace:
```
portcfg -ftrace [slot-number] ge port number [tunnel -id] cfg|del] <opt args>
```

To enable a trace:
1. Log on to the switch as admin.
2. Enter the `portcfg -ftrace` command with the following options:
   ```
   portcfg -ftrace ge0 cfg -a 0 -e 1
   ``
   This disables Auto Checkout and enables trace for GigE 0, tunnel 1

To delete a configuration for a tunnel:
1. Log on to the switch as admin.
2. Enter the `portcfg -ftrace` command with the following options:
   ```
   portcfg -ftrace ge1 1 del
   ``
   This deletes the configuration for tunnel 1.

### Displaying ftrace for a tunnel

The `portshow` command uses the `ftrace` option to display a trace for a tunnel.

Use the following syntax to display a trace:
```
portshow -ftrace [slot-number] ge port number [tunnel -id] cfg|del] <opt args>
```

To display the trace for a tunnel:
1. Log on to the switch as admin.
2. Enter the `portshow -ftrace` command with the following options:
   ```
   portshow -ftrace ge0 -stats
   ``
   This displays the trace stats for the GE port 0 for tunnel 1.

**NOTE:** The configuration file includes key FCIP FTRACE configuration values. Configurations are stored on a slot basis and not on blades, such as the FR4-18i. If the FR4-18i is swapped, the configuration stays the same for the new FR4-18i corresponding to the slot they are plugged in.

When performing a `configdownload`, the FCIP configuration is applied to the switch only on a slot power OFF or ON, for example slots containing the FR4-18i. The HP StorageWorks 400 MP Router, which is not slot based, requires a reboot. See the Fabric OS Command Reference for more information on any of these commands.

### Table 74  FTRACE configurable parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Range</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace Mask</td>
<td>0x8000</td>
<td>0-0xFFFFFFFF</td>
<td>Integer</td>
</tr>
<tr>
<td>Trigger Mask</td>
<td>0x00000003</td>
<td>0-0xFFFFFFFF</td>
<td>Integer</td>
</tr>
</tbody>
</table>

| NOTE: | The configuration file includes key FCIP FTRACE configuration values. Configurations are stored on a slot basis and not on blades, such as the FR4-18i. If the FR4-18i is swapped, the configuration stays the same for the new FR4-18i corresponding to the slot they are plugged in.

---

Fabric OS 6.x administrator guide  323
Recognizing port initialization and FCP auto discovery process

The steps in the port initialization process represent a protocol used to discover the type of connected device and establish the port type. The possible port types are as follows:

- **U_Port**—Universal FC port. The base Fibre Channel port type and all unidentified, or uninitiated ports are listed as U_Ports.
- **FL_Port**—Fabric Loop port. Connects both public and private loop devices.
- **G_Port**—Generic port. Acts as a transition port for non-loop fabric capable devices (E_Port / F_Port).
- **E_Port**—Expansion port.Assigned to ISL links.
- **F_Port**—Fabric port. Assigned to fabric capable devices.
- **EX_Port**—A type of E_Port. It connects a Fibre Channel router to an edge fabric. From the point of view of a switch in an edge fabric, an EX_Port appears as a normal E_Port. It follows applicable Fibre Channel standards as other E_Ports. However, the router terminates EX_Ports rather than allowing different fabrics to merge as would happen on a switch with regular E_Ports.
- **VE_Port**—Like an E_Port. However, it terminates at the switch and does not propagate fabric services or routing topology information from one edge fabric to another.
- **VEX_Port**—A type of VE_Port. It connects a Fibre Channel router to an edge fabric. From the point of view of a switch in an edge fabric, an VEX_Port appears as a normal VE_Port. It follows the same Fibre Channel protocol as other VE_Ports. However, the router terminates VEX_Ports rather than allowing different fabrics to merge as would happen on a switch with regular VE_Ports.

The FCP auto discovery process enables private storage devices that accept PRLI to communicate in a fabric.

If device probing is enabled, the embedded port PLOGIs and attempts a PRLI into the device to retrieve information to enter into the name server. This enables private devices that do not FLOGI but accept PRLI to be entered in the name server and receive full fabric citizenship. Private hosts require the QuickLoop feature which is not available in Fabric OS 4.0.0 and later.

A fabric-capable device will implicitly register information with name server during a FLOGI. These devices will typically register information with the name server before querying for a device list. The embedded port will still PLOGI and attempt PRLI with these devices.

You can view the name server table in Web Tools by clicking Name Server in the fabric toolbar. See the Web Tools Administrator’s Guide for more information.

Using port mirroring

Port mirroring lets you configure a switch port to connect to a port to mirror a specific source port and destination port traffic passing though any switch port. This is a useful way to troubleshoot without bringing down the host and destination links to insert an inline analyzer.

Port mirroring captures traffic between two devices. It mirrors only the frames containing the SID/DID to the mirror port. Because of the way it handles mirroring, a single mirror port can mirror multiple mirror connections. This also means that the port cannot exceed the maximum bandwidth of the mirror port. Attempts to mirror more traffic than available bandwidth result in the port mirror throttling the SID/DID traffic so that traffic does not exceed the maximum available bandwidth.

Port mirroring is supported between VE_Ports (VE_Port to VE_Port) with FCIP and no routing. The mirror port can be any port located on the same switch as the source identifier (SID).

Use port mirroring to detect missing frames, which may occur with zoning issues or hold timeouts, capture protocol errors, and capture ULP traffic (SCSI/FICON). This feature cannot be used on embedded switch traffic.

Port mirroring is only available using the FOS 5.2.0 or later CLI and is not available through Web Tools. For a complete list of port mirroring commands, see the Fabric OS Command Reference.

To ensure proper failover in HA configurations, both the active and the standby control processors (CP) must have firmware version 5.2.0 or later installed and running. If the OS on the standby CP does not support mirroring, failing over the standby CP could cause the HA failover to fail.
Supported hardware

Port mirroring is supported on Condor-based ASIC platforms, including:

- HP StorageWorks SAN Switch 4/32 and 4/32B
- HP StorageWorks 4/64 SAN Switch
- HP StorageWorks 400 MP Router
- 4/256 SAN Director and DC Director with chassis option 5

Port mirroring can be used on the following blades within a chassis:

- FC4-32 32-port blade
- FC4-16 16-port blade
- FC4-48 48-port blade
- FC8-16 16-port blade
- FC8-32 32-port blade
- FC8-48 48-port blade
- FC4-16IP iSCSI blade on FC ports only

The FC4-48 and FC8-48 implement port pairing, meaning that two ports share the same area. Port pairing uses a single area to map to two physical ports. A frame destined to the secondary port is routed to the primary port. The primary port’s filtering zone engine is used to redirect the frame to the secondary port. Port mirroring uses the port filter zone engine to redirect the frames to the mirror port. If two F_Ports share the same area, both ports cannot be part of a mirror connection. One of the two ports can be part of the connection as long as the other port is offline. Supported port configurations are shown in Table 75.

Table 75  Port combinations for port mirroring

<table>
<thead>
<tr>
<th>Primary port</th>
<th>Secondary port</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>F_Port</td>
<td>F_Port</td>
<td>No</td>
</tr>
<tr>
<td>F_Port</td>
<td>Offline</td>
<td>Yes</td>
</tr>
<tr>
<td>Offline</td>
<td>F_Port</td>
<td>Yes</td>
</tr>
<tr>
<td>F_Port</td>
<td>E_Port</td>
<td>Yes</td>
</tr>
<tr>
<td>E_Port</td>
<td>F_Port</td>
<td>Yes</td>
</tr>
<tr>
<td>E_Port</td>
<td>E_Port</td>
<td>No</td>
</tr>
</tbody>
</table>

If IOD is enabled, adding or deleting a port mirror connection causes a frame drop. Port mirroring reroutes a given connection to the mirror port, where the mirror traffic takes an extra route to the mirror port. When the extra route is removed, the frames between the two ports goes directly to the destination port. Since the frames at the mirror port could be queued at the destination port behind those frames that went directly to the destination port, port mirroring drops those frames from the mirror port when a connection is disabled. If IOD has been disabled, port mirroring does not drop any frames but displays an IOD error.

- A port cannot be mirrored to multiple locations. If you define multiple mirror connections for the same F_Port, all the connections must share the same mirror port.
- Local switches cannot be mirrored because FICON CUP frames to a local switch are treated as well-known addresses or embedded frame traffic.
- Using firmware download to downgrade to previous Fabric OS releases that do not support port mirroring requires that you remove all port mirroring connections.
Port mirroring considerations

Before creating port mirror connections, consider the following limitations:

- A mirror port can be any port on the same switch as the source identifier port.
- Only one domain can be mirrored per chip; after a domain is defined, only mirror ports on the defined domain can be used.

For example, in a three-domain fabric containing switches 4100A, 4100B, and 4100C, a mirror connection that is created between 4100A and 4100B only allows 4100A to add mirror connections for those ports on 4100B. To mirror traffic between 4100A and 4100C, add a mirror connection on 4100C. The first connection defines the restriction on the domain, which can be either the local domain or a remote domain.

- A switch that is capable of port mirroring can support a maximum of four mirror connections.

Each Field Description Block (FDB) defines an offset to search. Each offset can have up to four values that can be defined for a filter. If any of the four values match, the filter will match.

- Mirror port bandwidth limits mirror connections.

The bandwidth of the mirror port is unidirectional. The host (SID) talks to multiple storage devices (DIDs) and does not send full line rate to a single target. A mirror port configured at 2Gb can only support up to 2Gb of traffic. A normal 2G F_Port is bidirectional and can support up to 4Gb of traffic (two to transmit and two to receive). If the mirror port bandwidth is exceeded, the receiver port is not returned any credits and the devices in the mirror connection see degraded performance.

- Deleting a port mirroring connection with In Order Deliver (IOD) enabled causes frame drop between two endpoints.

- Using the firmware download procedure to downgrade to previous Fabric OS releases that do not support port mirroring requires that you remove all the port mirroring connections. If you downgrade to a previous versions of Fabric OS, you cannot proceed until the mirroring connections are removed.

Creating, deleting, and displaying port mirroring

The method for adding a port mirror connection between two local switch ports and between a local switch port and a remote switch port is the same. First you must configure a port to be a mirror port before you can perform a `portMirror --add`, or `portMirror --delete`.

To configure a port to be a mirror port:

- Type `portcfg mirrorport slot/port --enable`.

**NOTE:** The `enable` command enables the port as mirror port. The `disable` command disables the mirror port configuration.

To add a port mirror connection:

1. Log in to the switch as admin.
2. Type `portMirror --add slotnumber/portnumber SourceID DestID`.

**NOTE:** The lower 8 bits of the address is ignored. For example, the ALPA for loop devices.

The configuration database keeps information about the number of port mirror connections configured on a switch, the number of chunks of port mirroring data that are stored, and the chunk number. When removing a mirror connection, always use this method to ensure that the data is cleared. Deleting a connection removes the information from the database.
To delete a port mirror connection between two local switch ports or a local and a remote switch port:

1. Log in to the switch as admin.
2. Type `portMirror --del SourceID DestID`.
   For example, to delete the port mirror connection on mirror port 2, you might type:
   ```
   portMirror -del 0x011400 0x240400
   ```

To display port mirror connections:

1. Log in to the switch as admin.
2. Type `portMirror --show`.
   You should see output similar to the following:
   ```
   switch:admin> portmirror --show
   Number of mirror connection(s) configured: 4

   Mirror_Port  SID       DID       State
   -------------------------------
   18           0x070400  0x0718e2  Enabled
   18           0x070400  0x0718e3  Enabled
   18           0x070400  0x0718ef  Enabled
   18           0x070400  0x0718e0  Enabled
   ```

   The `switchShow` command output shows the mirror port as shown in the following example.
   ```
   switch:admin> switchshow
   switchName:     ABCD
   switchType:     26.1
   switchState:    Online
   switchMode:     Native
   switchRole:     Principal
   switchDomain:   1
   switchId:       fffc01
   switchWwn:      10:00:00:05:1e:34:00:70
   zoning:         OFF
   switchBeacon:   OFF

   Area Port Media Speed State       Proto
   -------------------------------
   0   0   id    N2   In_Sync
   1   1   id    N2   Online     F-Port  21:00:00:e0:8b:13:08:10
   2   2   id    N2   No_Light
   3   3   --    N2   No_Module
   4   4   --    N2   No_Module
   5   5   id    N2   No_Light
   6   6   --    N2   No_Module
   7   7   --    N2   No_Module
   8   8   id    N2   No_Light
   9   9   id    N2   No_Light
   10  10  --    N2   No_Module
   11  11  --    N2   No_Module
   ```
12  12  --  N2  No_Module
13  13  --  N2  No_Module
14  14  id  N2  Online           F-Port  21:00:00:e0:8b:12:8a:be
15  15  id  N2  Online           E-Port  segmented,(No Fabric License)
15 Administering NPIV

This chapter describes the concepts and procedures for administering N-Port ID Virtualization (NPIV).

About NPIV

NPIV enables a single Fibre Channel protocol port to appear as multiple, distinct ports, providing separate port identification within the fabric for each operating system image behind the port (as if each operating system image had its own unique physical port). NPIV assigns a different virtual port ID to each Fibre Channel protocol device. NPIV is designed to enable you to allocate virtual addresses without impacting your existing hardware implementation. The virtual port has the same properties as an N_Port, and is therefore capable of registering with all services of the fabric.

Each NPIV device has a unique device PID, Port WWN, and Node WWN, and should act the same as all other physical devices in the fabric; in other words, multiple virtual devices emulated by NPIV appear no different than regular devices connected to a non-NPIV port. The same zoning rules apply to NPIV devices as non-NPIV devices. Zones can be defined by domain,port notation, by WWN zoning, or both. To perform zoning to the granularity of the virtual N_Port IDs, you must use WWN-based zoning.

If you are using domain,port zoning for an NPIV port, and all the virtual PIDs associated with the port are included in the zone, then a port login (PLOGI) to a non-existent virtual PID is not blocked by the switch; rather, it is delivered to the device attached to the NPIV port. In cases where the device is not capable of handling such unexpected PLOGIs, you should use WWN-based zoning.

Enabling and disabling NPIV

The SAN Switch 4/32, SAN Switch 4/32B, 4/64 SAN Switch NPIV is enabled for every port.

**NOTE:** Director blade FC10-6 does not support NPIV.

To enable or disable NPIV on a port-by-port basis, enter the `portCfgNPIVPort` command.

The following example shows NPIV being enabled on port 10 of a SAN Switch 4/32:

```
switch:admin> portCfgNPIVPort 10, 1
```

Configuring NPIV

To specify the number of virtual N_Port IDs per port or per switch, use the `configure` command with either of the following parameters:

- `switch.login.perPortMax`
  
  Use this parameter to set the number of virtual N_Port IDs per port to a value between 0 and 255. The default setting is 126.

  **For the 4/256 SAN Director with an FC4-48 or the DC SAN Backbone Director (short name, DC Director) with an FC8-48 port blade:** For ports 0 through 15 on the FC4-48 and FC8-48 port blade, the maximum number of virtual N_Port IDs per port is 255; for ports 16 through 47, the maximum number is 127.

- `switch.login.perSwitchMax`
  
  Use this parameter to set the number of virtual N_Port IDs per switch to a value between 0 and 126 multiplied by the `<number of ports>`. The default setting is 15 multiplied by the `<number of ports>`.
The following example shows the configuration of these parameters:

switch:admin> switchdisable
switch:admin> configure

Configure...

Fabric parameters (yes, y, no, n): [no]
Virtual Channel parameters (yes, y, no, n): [no]
F-Port login parameters (yes, y, no, n): [no] y

Maximum logins per switch: (1..4032) [4032] 2048
Maximum logins per port: (1..255) [255] 126

switch:admin> switchenable

Configuration scenarios

The actual number of virtual N_Port IDs accepted per port and per switch is determined by the limits you set, and also by the limit that is reached first.

For example, if you’ve set switch.login.perPortMax to 25, and switch.login.perSwitchMax to 100, then the first 4 ports will accept 25 virtual N_Port IDs each. However, the fifth port will reject any more virtual N_Port IDs because the switch.login.perSwitchMax parameter (100) has been reached.

If you set switch.login.perPortMax to 50, and switch.login.perSwitchMax to 25, then the first port requests 50 virtual N_Port IDs; 25 are accepted, and 25 are rejected. The second port requests 50 virtual N_Port IDs, but none are accepted, because the switch.login.perSwitchMax limit of 25 has been reached.

Viewing NPIV port configuration information

To view the NPIV capability of switch ports, enter the portcfgshow command. The following example shows whether or not a port is configured for NPIV:

switch:admin> portcfgshow
Ports of Slot 0  0  1  2  3  4  5  6  7  8  9  10  11  12  13  14  15
---------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+--
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
RSCN Suppressed   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON

Use the switchShow and portShow commands to view NPIV information for a given port. If a port is an F_Port, and you enter the switchShow command, then the port WWN of the N_Port is returned. For an NPIV F_Port, there are multiple N_Ports, each with a different port WWN. The switchShow command
output indicates whether or not a port is an NPIV F_Port, and identifies the number of virtual N_Ports behind it. Following is sample output from the `switchShow` command:

```
switch: admin> switchshow
switchName: swd77
switchType: 32.0
switchState: Online
switchMode: Native
switchRole: Principal
switchDomain: 99
switchId: fff6c63
switchWwn: 10:00:00:05:1e:35:37:40
zoning: OFF
switchBeacon: OFF

Area  Port  Media  Speed  State
-----------------------------
 0   0   id    N2   Online    F-Port  50:05:07:64:01:20:73:b8
 1   1   id    N2   Online    F-Port  50:05:07:64:01:60:73:b8
 2   2   id    N2   Online    F-Port  65 NPIV public
 3   3   id    N2   Online    F-Port  50:05:07:64:01:e0:73:b8
 4   4   id    N2   Online    F-Port  50:05:07:64:01:20:73:b5
...<output truncated>
```

Use the `portShow` command to view the NPIV attributes and all the N_Port (physical and virtual) port WWNs under “portWwn of device(s) connected.” Following is sample output for the `portShow` command:

```
switch: admin> portshow 2
portName: 02
portHealth: HEALTHY
Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x24b03 PRESENT ACTIVE F_PORT G_PORT NPIV LOGICAL_ONLINE LOGIN NOELP LED ACCEPT
portType: 10.0
portState: 1Online
portPhys: 6In_Sync
portScn: 32F_Port
port generation number: 148
portId: 630200
portIfId: 43020005
portWwn: 20:02:00:05:1e:35:37:40
portWwn of device(s) connected:
c0:50:76:ff:fb:00:16:fc
c0:50:76:ff:fb:00:16:f8
...
Displaying login information

Use the `portLoginShow` command to display the login information for the virtual PIDs of a port. Following is sample output from the `portLoginShow` command:

```
switch:admin> portloginshow 2
Type  PID     World Wide Name        credit df_sz cos
c-----------------------------------------------
fe  630240  c0:50:76:ff:fb:00:16:fc   101  2048   c  scr=3
fe  63023f  c0:50:76:ff:fb:00:16:f8   101  2048   c  scr=3
fe  63023e  c0:50:76:ff:fb:00:17:ec   101  2048   c  scr=3
...<output truncated>
...ff  630202  c0:50:76:ff:fb:00:17:70  192  2048   c  d_id=FFFFFC
ff  630201  c0:50:76:ff:fb:00:16:80  192  2048   c  d_id=FFFFFC
```
16 Optimizing fabric behavior

This chapter describes the Adaptive Networking features.

Introduction to adaptive networking

Adaptive Networking is a suite of tools and capabilities that enable you to ensure optimized behavior in the SAN. Even under the worst congestion conditions, the Adaptive Networking features can maximize the fabric behavior and provide necessary bandwidth for high-priority, mission-critical applications and connections.

The following sections cover three features in the Adaptive Networking suite: Traffic Isolation, QoS Ingress Rate Limiting, and QoS SID/DID Traffic Prioritization.

Top Talkers, which is another Adaptive Networking feature, is described briefly in this chapter and described in detail in “Administering Advanced Performance Monitoring” on page 361.

Top Talkers

The Top Talkers feature provides real-time information about the top “n” bandwidth-consuming flows from a set of a large number of flows passing through a specific port in the network. You can use Top Talkers to identify the SID/DID pairs that consume the most bandwidth and can then configure them with certain QoS attributes so they get proper priority.

The Top Talker feature is part of the optionally licensed Advanced Performance Monitoring feature. See “Identifying top bandwidth users (Top Talkers)” on page 370 for detailed information about Top Talkers.

Traffic Isolation

The Traffic Isolation feature allows you to control the flow of interswitch traffic by creating a dedicated path for traffic flowing from a specific set of source ports (N_Ports). For example, you might use Traffic Isolation for the following scenarios:

- To dedicate an ISL to high priority, host-to-target traffic.
- To force high volume, low priority traffic onto a given ISL to limit the effect on the fabric of this high traffic pattern.

Traffic Isolation is implemented using a special zone, called a Traffic Isolation zone (TI zone). A TI zone indicates the set of N_Ports and E_Ports to be used for a specific traffic flow. When a TI zone is activated, the fabric attempts to isolate all inter-switch traffic entering from a member of the zone to only those E_Ports that have been included in the zone. The fabric also attempts to exclude traffic not in the TI zone from using E_Ports within that TI zone.

Figure 21 shows a fabric with a TI zone consisting of N_Ports “1,8” and “4,6” and E_Ports “1,1”, “3,9”, “3,12”, and “4,7”. The dotted line indicates the dedicated path from Domain 1 to Domain 4.

Figure 21 Traffic Isolation zone creating a dedicated path through the fabric
In Figure 21, all traffic entering Domain 1 from N_Port 8 is routed through E_Port 1. Similarly, traffic entering Domain 3 from E_Port 9 is routed to E_Port 12, and traffic entering Domain 4 from E_Port 7 is routed to the device through N_Port 6. Traffic coming from other ports in Domain 1 would not use E_Port 1, but would use E_Port 2 instead.

Other traffic is excluded from the dedicated path as long as other equal-cost routes through the fabric exist. For example, if the ISL formed by E_Ports “1,2” and “3,10” failed, all traffic between Domains 1 and 3 would use the ISL formed by E_Ports “1,1” and “3,9”, even though that ISL is a dedicated path in a TI zone.

Use the zone command to create and manage TI zones. Refer to the Fabric OS Command Reference for details about the zone command.

**TI zone failover**

A TI zone can have failover enabled or disabled. If the dedicated path cannot be used and failover is enabled, the TI zone traffic will use a non-dedicated path instead. If the dedicated path cannot be used and failover is disabled, the Traffic Isolation path is broken and traffic for that TI zone is halted until the dedicated path is fixed.

For example, in Figure 21, if the dedicated ISL between Domain 1 and Domain 3 goes offline, then the following occurs, depending on the failover option:

- If failover is enabled for the TI zone, the traffic is routed from Domain 1 to Domain 3 through E_Ports “1,2” and “3,10”.
- If failover is disabled for the TI zone, the traffic is halted until the ISL between Domain 1 and Domain 3 is back online.

**FSPF routing rules and Traffic Isolation**

FSPF routing rules take precedence over the TI zones, as described in the following situations:

- If other paths through the fabric exist, but they are not the shortest path, then traffic uses the dedicated ISL.
- If a TI zone creates a path that is not the lowest cost path and failover is enabled, the lowest cost path is used instead. If failover is not enabled, the traffic path for the TI zone is broken.

For example, in Figure 22, there is a dedicated path between Domain 1 and Domain 3, and another, non-dedicated, path that passes through Domain 2. Since the non-dedicated path is not the shortest path between Domain 1 and Domain 3, all traffic will use the dedicated path.

**Figure 22** Dedicated path (shortest path)
In Figure 23, a dedicated path between Domain 1 and Domain 4 exists, but is not the shortest path. In this situation, if failover is enabled, the TI zone traffic uses the shortest path, even though the E_Ports are not in the TI zone. If failover is disabled, the TI zone traffic stops until the dedicated path is configured to be the shortest path.

**General rules for TI zones**

Note the following general rules for TI zones:

- A given N_Port can be a member of only a single TI zone. This rule is enforced during zone creation or modification.
- An E_Port can be a member of only a single TI zone. The same checking is done as described for N_Ports.

If multiple E_Ports are configured that are on the lowest cost route to a domain, the various source ports for that zone are load-balanced across the specified E_Ports.

- The TI zones appear in the defined zone configuration only and do not appear in the effective zone configuration. A TI zone only provides Traffic Isolation and is not a “regular” zone.
- A TI zone must include a set (two or more) of E_Ports forming an end-to-end path. Inclusion of N_Ports is optional.
- Each TI zone is interpreted by each switch and each switch considers only the routing required for its local ports. No consideration is given to the overall topology and to whether the TI zones accurately provide dedicated paths through the whole fabric.

For example, in Figure 24, the TI zone was configured incorrectly and E_Port “3,9” was erroneously omitted from the zone. The domain 3 switch assumes that traffic coming from E_Port 9 is not part of the TI zone and so that traffic is routed to E_Port 11 instead of E_Port 12, if failover is enabled. If failover is disabled, the route is broken and traffic stops.

- You create and modify TI zones using the `zone` command. Other zoning commands, such as `zoneCreate`, `aliCreate`, and `cfgCreate`, cannot be used to manage TI zones.
Supported configurations for Traffic Isolation

Note the following configuration rules for TI zones:

- Traffic Isolation is supported only on the HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, and 400 Multi-protocol Router, 4/256 SAN Director and DC SAN Backbone Director (short name, DC Director), all configured in Brocade Native Mode (interopmode 0).
- Traffic Isolation has limited support for FICON FCIP in McDATA Fabric Mode (interopmode 2), in the following configuration only:

  - 400 Multi-protocol Router with E_Port connections to an M-switch and VE_Port connections to another 400 Multi-protocol Router.
  - Devices attached to M-switch only.
  - Traffic Isolation is not supported in fabrics configured in Open Fabric Mode (interopmode 3).
  - Limited USD-X replacement support for FICON FCIP in McDATA Fabric Mode.
  - 400 Multi-protocol Router (platform specific) with E-port connections to an M-switch and VE-port connections to another 400 Multi-protocol Router.
  - Devices attached to M-switch only.

This feature is not supported in fabrics configured in any interopMode except for a predefined FICON FCIP configuration in McDATA Fabric Mode.

- VE_Ports are supported in TI zones.
- FCR does not support Traffic Isolation.
- Ports in a TI zone must belong to switches that run Fabric OS v6.0 or later.
- Traffic Isolation is not supported in fabrics with switches running firmware versions earlier than Fabric OS 6.0. However, the existence of a TI zone in such a fabric is backward compatible and does not disrupt fabric operation in switches running earlier firmware versions.
Limitations and restrictions of Traffic Isolation

The following are limitations of TI zones:

- A maximum of 255 TI zones can be created in one fabric. A fabric merge resulting in greater than 255 TI zones results in merge failure and the fabrics are segmented.
- A TI zone can be created using D,I (Domain, Index) notation only. Use of WWNs is not allowed.
- To include a trunk group in a TI zone, you must include all ports of the trunk in the TI zone.
- Two N_Ports that have the same shared area cannot be configured in different TI zones. This limitation does not apply to E_Ports that use the same shared area.
- Ports that are in different TI zones cannot communicate with each other if failover is disabled, even if they are in the same (regular) zone.

Admin Domain considerations for Traffic Isolation

Note the following if you implement Admin Domains and TI zones:

- TI zones are applicable only in AD0, and the E_Ports that are members of a TI zone must be in the AD0 device list. Because TI zones must use D,I notation, the AD0 device list must be declared using D,I notation for ports that are to be used in TI zones.
- A port used in a TI zone cannot be a member of multiple Admin Domains.
- Use care if defining TI zones with ports that are shared across Admin Domains because of the limitation that a given port can appear in only one TI zone. Use the zone --validate command to detect conflicting members across Admin Domains.

Best practice: Do not use ports that are shared across Admin Domains in a TI zone.

Creating a TI zone

When you create a TI zone, by default, failover is enabled and the zone is activated.

To create a TI zone:

1. Connect to the switch and log in as admin.
2. Enter the zone --create command.

   ```shell
   zone --create -t ti objtype [-o optlist] name -p "portlist"
   ```

   where:

   - **objtype** The zone object type, which is `ti` for TI zones.
   - **optlist** A list of options for creating the zone and controlling failover mode.
     - Activate the zone after it is created.
     - Deactivate the zone after it is created.
     - Disable failover mode.
     - Enable failover mode.
   - **name** The name of the zone to be created.
   - **portlist** The list of ports to be included in the TI zone. Ports are designated using “D,I” (Domain,Index) format. Multiple ports are separated by a semicolon, followed by a space.

3. Enter the cfgEnable command for the appropriate zone configuration to make the change effective.

The following examples create a TI zone named “redzone”, which contains E_Ports 1,1 and 2,4 and N_Ports 1,8 and 2,6.

To create a TI zone with failover enabled and activate it (default settings), type:

   ```shell
   zone --create -t ti redzone -p "1,1; 2,4; 1,8; 2,6"
   ```

To create a deactivated TI zone with failover disabled, type:

   ```shell
   zone --create -t ti -o dn redzone -p "1,1; 2,4; 1,8; 2,6"
   ```
Modifying TI zones

Using the `zone --add` and `zone --remove` commands, you can add and remove ports and change the failover option of existing TI zones.

If you remove the last member of a TI zone, the TI zone is deleted.

To modify a TI zone:

1. Connect to the switch and log in as admin.
2. Enter the `zone --add` command to add ports or change the failover option for an existing TI zone. Enter the `zone --remove` command to remove ports from an existing TI zone.

```
zone --add [-o optlist] name -p "portlist"
```

```
zone --remove name -p "portlist"
```

where:

- **optlist**: A list of options for controlling failover mode.
  - Disable failover mode.
  - Enable failover mode.
- **name**: The name of the zone to be modified.
- **portlist**: The list of ports to be added to or removed from the TI zone. Ports are designated using "D,I" (Domain,Index) format. Multiple ports are separated by a semicolon, followed by a space.

3. Enter the `cfgEnable` command for the appropriate zone configuration to make the change effective.

To add port members to the existing TI zone redzone, type:

```
zone --add "redzone" -p "3,4; 3,6"
```

To disable failover on the existing TI zone redzone, type:

```
zone --add -o n "redzone"
```

To enable failover and add ports to TI zone greenzone, type:

```
zone --add -o f "greenzone" -p "3,4"
```

To remove ports from the TI zone redzone, type:

```
zone --remove "redzone" -p "3,4; 3,6"
```

### Activating and deactivating a TI zone

The TI zone must exist before you can activate it. To activate or deactivate a TI zone:

1. Connect to the switch and log in as admin.
2. Enter the `zone --activate` command to activate a TI zone. Enter the `zone --deactivate` command to deactivate a TI zone.

```
zone --activate name
```

```
zone --deactivate name
```

where:

- **name**: The name of the zone to be activated or deactivated.

3. Enter the `cfgEnable` command for the appropriate zone configuration to make the change effective.

To activate the existing TI zone redzone, type:

```
zone --activate redzone
```

To deactivate the existing TI zone greenzone, type:

```
zone --deactivate "greenzone"
```
Deleting a TI zone

Use the `zone --delete` command to delete a TI zone from the defined configuration. This command deletes the entire zone; to only remove port members from a TI zone, use the `zone --remove` command, as described in “Modifying TI zones” on page 337.

To delete a TI zone:

1. Connect to the switch and log in as admin.
2. Enter the `zone --delete` command.
   
   ```
   zone --delete name
   ```
   
   where:
   
   name The name of the zone to be deleted.

   You can delete multiple zones by separating the zone names with a semicolon and enclosing them in quotation marks.

3. Enter the `cfgEnable` command for the appropriate zone configuration to make the change effective.

   To delete the TI zone `redzone`, type:
   ```
   zone --delete redzone
   ```

Displaying TI zones

Use the `zone --show` command to display information about TI zones. This command displays the following information for each zone:

- zone name
- E_Port members
- N_Port members
- failover option (enabled or disabled)
- zone status (activated or deactivated)

To display information about TI zones:

1. Connect to the switch and log in as admin.
2. Enter the `zone --show` command.
   
   ```
   zone --show [ name ]
   ```
   
   where:
   
   name The name of the zone to be displayed. If the name is omitted, the command displays information about all TI zones in the defined configuration.

   To display information about the TI zone `redzone`, type:
   ```
   zone --show redzone
   ```

   To display information about all TI zones, type:
   ```
   zone --show
   ```

QoS: ingress rate limiting

Ingress rate limiting is a licensed feature that restricts the speed of traffic from a particular device. Use ingress rate limiting for the following situations:

- To reduce existing congestion in the network or proactively avoid congestion.
- To enable you to offer flexible bandwidth limit services based on requirements.
- To enable more important devices to use the network bandwidth during specific services, such as network backup.
To limit the traffic, you set the maximum speed at which the traffic can flow through a particular F_Port or FL_Port. For example, if you set the rate limit at 4 Gbps, then traffic from a particular device is limited to a maximum of 4 Gbps.

Ingress rate limiting enforcement is needed only if the port can run at a speed higher than the rate limit. For example, if the rate limit is 4 Gbps and the port is only a 2 Gbps port, then ingress rate limiting is not enforced.

Ingress rate limiting is applicable only to F_Ports and FL_Ports and is available only on the DC Director model. The ingress rate limiting configuration is persistent across reboots.

To limit traffic from a particular device:

1. Connect to the switch and log in as admin.
2. Enter the `portcfgqos --setratelimit` command.
   
   ```
   portcfgqos --setratelimit [slot/]port ratelimit
   ```

   where:
   - `slot/port`: The slot and port number of the F_Port or FL_Port on which you want to limit traffic. The slot number is required for a 4/256 SAN Director or DC Director.
   - `ratelimit`: The maximum speed, in megabits per second (Mbps), for traffic coming from the device. The valid values are: 200, 400, 600, 800, 1000, 1500, 2000, 2500, 3000, 3500, 4000, 5000, 6000, 7000, and 8000.

   For example, to set the rate limit on slot 3, port 9 to 4000 Mbps, enter the following command:
   
   ```
   portcfgqos --setratelimit 3/9 4000
   ```

To disable ingress rate limiting:

1. Connect to the switch and log in as admin.
2. Enter the `portcfgqos --resetratelimit` command.
   
   ```
   portcfgqos --resetratelimit [slot/]port
   ```

   where:
   - `slot/port`: The slot and port number of the F_Port or FL_Port for which you want to disable ingress rate limiting. The slot number is required for a 4/256 SAN Director or DC Director.

   For example, to disable ingress rate limiting on slot 3, port 9, enter the following command:
   
   ```
   portcfgqos --resetratelimit 3/9
   ```

**QoS: SID/DID traffic prioritization**

SID/DID traffic prioritization is a licensed feature that allows you to categorize the traffic flow between a given host and target as having a high or low priority. For example, you could assign online transaction processing (OLTP) to high priority and backup traffic to low priority.

All flows without QoS prioritization are considered medium priority.

High, medium, and low priority flows are allocated to different virtual channels (VCs). High priority flows receive more VCs than medium priority flows, which receive more VCs than low priority flows.

> **NOTE:** If there is a single low priority flow to a destination ID (DID) and several medium priority flows to that same DID, then it is possible that the medium priority flows would have less bandwidth because they have to share the medium priority VCs, whereas the low priority flow would have a separate VC.

SID/DID traffic prioritization is a licensed feature. An Adaptive Networking license must be installed on every switch that is in the path between a given configured device pair.
QoS zones

You assign high or low priority (QoS level) using a QoS zone. A QoS zone is a special zone that indicates the priority of the traffic flow between a given host/target pair. The members of a QoS zone are WWNs of the host/target pairs. QoS zones can contain only WWN members. “Domain,Index” zoning is not supported.

A QoS zone has a special name, to differentiate it from a regular zone. The format of the QoS zone name is as follows:

\[ \text{QOS}p_{-}xxxxxx \]

where \( p \) is the priority level (H for High or L for Low) and \( xxxxx \) is the user-defined portion of the name. For example, the following are valid QoS zone names:

- QOSH_HighPriorityTraffic
- QOSL_LowPriorityZone

The switch automatically sets the priority for the “host,target” pairs specified in the zones based on the priority level in the zone name.

For example, Figure 25 shows a fabric with two hosts (H1, H2) and three targets (S1, S2, S3). The traffic prioritization is as follows:

- Traffic between H1 and S1 is high priority.
- Traffic between H1 and S3 and between H2 and S3 is low priority.
- All other traffic is medium priority, which is the default.

\[ \text{QOS}H_{-}\text{Zone1 Members: H1, S1} \]
\[ \text{QOS}L_{-}\text{Zone3 Members: H1, H2, S3} \]

Figure 25  QoS traffic prioritization

For this fabric, you could set up the following QoS zones:

- QOSH_Zone1  Members: H1, S1
- QOSL_Zone3  Members: H1, H2, S3
**QoS on E_Ports**

In addition to configuring the hosts and targets in a zone, you must also enable QoS on individual E_Ports that might carry traffic between the given host and target pairs. Path selection between the “host,target” pairs is governed by FSPF rules and is not affected by QoS priorities. By default, QoS is enabled on E_Ports in port configuration. For example, in Figure 26, QoS should be enabled on the encircled E_Ports.

![Figure 26 QoS with E_Ports enabled](image)

You need to enable QoS on the E_Ports on both ISLs between Domain 3 and Domain 4 because either path might be selected to carry the traffic.

You do not need to enable QoS on the E_Ports on the ISLs between Domain 1 and Domain 2 and between Domain 2 and Domain 3, because these are not the shortest paths between the hosts and the targets. However, if the ISL between Domain 1 and Domain 3 is broken, then the path through Domain 2 would be used.

To guarantee traffic priority, you should enable QoS on all possible E_Ports. Alternatively, you could use a TI zone to limit the E_Ports that carry the traffic between a “host,target” pair and enable QoS on only those E_Ports.

If QoS is not enabled on an E_Port, the traffic prioritization stops at that point. For example, in Figure 26 if you disabled QoS on E_Ports “3,12” and “3,13” then the traffic from H1 and H2 to S3 would be low priority from the hosts to Domain 3, but would switch to the default (medium) priority from Domain 3 to the target S3.

**Supported configurations for traffic prioritization**

Note the following configuration rules for traffic prioritization:

**IMPORTANT:** All switches in the fabric must be running Fabric OS 6.0.0 or higher. If QoS traffic crosses an ISL for a switch running an earlier firmware version, the frames are dropped.

- By default, all devices are assigned medium priority. To be assigned high or low priority, hosts and targets must be connected to a DC Director. To preserve the priority level across ISLs, the switches must be running Fabric OS 6.0.0 or later and must be one of the following: HP StorageWorks SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, 4/256 SAN Director, or DC Director.

- If a host and target are included in two or more QoS zones with different priorities, the zone with the lowest priority takes precedence. For example, if an effective zone configuration has QOSH_z1 (H,T) and QOSL_z2 (H,T), the traffic flow between H and T will be of low QoS priority. Additionally, if QOSH_z1 (H,T) overlaps with a “domain,port” zone at the H port, the traffic flow between H and T is dropped to medium priority and the H port is marked as a session-based soft zoning port.

- Traffic prioritization is not supported on 10 Gbps ISLs.
• Traffic prioritization is not supported on mirrored ports.

**Traffic prioritization**

1. Connect to the switch and log in as admin.
2. Enter the `zoneCreate` command, using the following syntax:
   
   ```
   zonecreate "QOSP_zonename", "member[; member...]"
   ```
   
   where:
   
   - **p** The priority of the traffic. Possible values are:
     - HHigh priority
     - LLCow priority
   - **zonenumber** The user-defined part of the name of the zone to be created.
   - **member** A member or list of members to be added to the zone. A zone member must be specified using WWN only.

3. Enter the `cfgAdd` command to add the QoS zone to the zone configuration, using the following syntax:
   
   ```
   cfgadd "cfgname", "QOSP_zonename"
   ```
   
   where:
   
   - **cfgname** The name of the zone configuration.
   - **QOSP_zonename** The name of the QoS zone to be added to the configuration.

4. Enter the `cfgSave` command to save the change to the defined configuration.
5. Enter the `cfgEnable` command for the appropriate zone configuration to make the change effective.
   
   ```
   cfgenable "cfgname"
   ```
   
   where:
   
   - **cfgname** The name of the zone configuration.

6. Enter the `portCfgQos` command to enable QoS on the E_Ports, using the following syntax:
   
   ```
   portcfgqos --enable [slot/]port
   ```
   
   where:
   
   - **slot/port** The slot and port number of the E_Port on which you want to enable QoS. The slot number is required for a 4/256 SAN Director or DC Director.
17 Administering Advanced Performance Monitoring

This chapter contains information about the Advanced Performance Monitoring licensed feature.

About Advanced Performance Monitoring

Based on Frame Filtering technology and a unique performance counter engine, Advanced Performance Monitoring is a comprehensive tool for monitoring the performance of networked storage resources. Advanced Performance Monitoring provides the following monitors:

- **End-to-End monitor** — Measures the traffic between a host/target pair.
- **Filter-based monitor** — Measures the traffic transmitted through a port with specific values in the first 64 bytes of the frame.
- **ISL monitoring** — Measures the traffic transmitted through an InterSwitch Link (ISL) to different destination domains.
- **AL_PA monitoring** — Reports cyclic redundancy check (CRC) error measurement statistics for an AL_PA.
- **Top Talker monitoring** — Measures the flows that are major consumers of bandwidth on a port.

**NOTE:** Advanced Performance Monitoring is not supported on VE_Ports (virtual FC_Ports) and EX_Ports. If you issue commands for any Advanced Performance Monitors on VE_Ports or EX_Ports you will receive error messages. See “Configuring and Monitoring FCIP Extension Services” on page 435 for more information about VE_Ports.

Additional performance monitoring features are provided through Web Tools. For additional information, see the Web Tools Administrator’s Guide.

The type of monitors supported depends on the ASIC. Table 76 shows the monitors supported on different ASICS.

**Table 76** Types of monitors supported on Brocade switch models

<table>
<thead>
<tr>
<th>Monitors:</th>
<th>EE</th>
<th>Filter</th>
<th>ALPA</th>
<th>ISL</th>
<th>Top Talker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goldeneye ASIC (Brocade 4/8 SAN Switch, 4/16 SAN Switch)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Condor ASIC (SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, and the 4/256 SAN Director)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Condor2 ASIC DC SAN Backbone Director (short name, DC Director)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Bloom ASIC</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**NOTE:** The HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, 4/256 SAN Director and DC Director switches do not display AL_PA measurements for end-to-end monitors. CRC reports are accessed using Web Tools.

Also, AL_PA monitoring is not supported on NPIV configured ports.
Table 77 lists commands associated with Advanced Performance Monitoring. Advanced Performance Monitor commands are available only to users with the admin or switchAdmin roles. For detailed information on these commands, see the Fabric OS Command Reference.

Table 77  Advanced Performance Monitoring commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>perfAddEEMonitor</td>
<td>Add an end-to-end monitor to a port.</td>
</tr>
<tr>
<td>perfAddIPMonitor</td>
<td>Add an IP monitor to a port.</td>
</tr>
<tr>
<td>perfAddReadMonitor</td>
<td>Add a SCSI Read monitor to a port.</td>
</tr>
<tr>
<td>perfAddRwMonitor</td>
<td>Add a SCSI Read and Write monitor to a port.</td>
</tr>
<tr>
<td>perfAddSCSIMonitor</td>
<td>Add a SCSI traffic frame monitor to a port.</td>
</tr>
<tr>
<td>perfAddUserMonitor</td>
<td>Add a filter-based monitor to a port.</td>
</tr>
<tr>
<td>perfAddWriteMonitor</td>
<td>Add a SCSI Write monitor to a port.</td>
</tr>
<tr>
<td>perfCfgClear</td>
<td>Clear the performance monitoring settings from nonvolatile (flash) memory.</td>
</tr>
<tr>
<td>perfCfgRestore</td>
<td>Restore performance monitoring settings from nonvolatile (flash) memory.</td>
</tr>
<tr>
<td>perfCfgSave</td>
<td>Save the current performance monitoring settings to nonvolatile (flash) memory.</td>
</tr>
<tr>
<td>perfClearAlpaCrc</td>
<td>Clear an AL_PA device CRC count by the port and AL_PA.</td>
</tr>
<tr>
<td>perfClearFilterMonitor</td>
<td>Clear filter-based monitor counters.</td>
</tr>
<tr>
<td>perfDelEEMonitor</td>
<td>Delete an end-to-end monitor on a port.</td>
</tr>
<tr>
<td>perfDelFilterMonitor</td>
<td>Delete a filter-based monitor.</td>
</tr>
<tr>
<td>perfMonitorClear</td>
<td>Clear statistics counters of end-to-end, filter-based, and ISL monitors on a port.</td>
</tr>
<tr>
<td>perfMonitorShow</td>
<td>Display end-to-end, filter-based, and ISL monitors on a port.</td>
</tr>
<tr>
<td>perfSetPortEEMask</td>
<td>Set overall mask for end-to-end (EE) monitors.</td>
</tr>
<tr>
<td>perfShowAlpaCrc</td>
<td>Display the AL_PA CRC count by port or by AL_PA.</td>
</tr>
<tr>
<td>perfShowEEMonitor</td>
<td>Show user-defined end-to-end monitors.</td>
</tr>
<tr>
<td>perfttmon</td>
<td>Add, delete, or display Top Talker monitors.</td>
</tr>
</tbody>
</table>

**NOTE:** The command examples in this chapter use the slot/port syntax required by 4/256 SAN Director and DC Directors. For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, and the 400 Multi-protocol Router, use only the port number where needed in the commands.
Monitoring AL_PAs

You can use the `perfShowAlpaCrc` command to display the CRC error count for all AL_PA devices or for a single AL_PA on a specific active L_Port.

The following example displays the CRC error count for all AL_PA devices on a port:

```bash
switch:admin> perfshowalpacrc 1/1
AL_PA   CRC count
---------
0xd9    0
```

The following example displays the CRC error count for a single AL_PA device on a port:

```bash
switch:admin> perfshowalpacrc 1/1, 0xd9
The CRC count at ALPA 0xd9 on port 1 is 0x000000000.
```

The following example clears the CRC error count:

```bash
switch:admin> perfclearalpacrc 1/1, 0xd9
CRC error count at AL_PA 0xd9 on port 1 is cleared.
switch:admin> perfclearalpacrc 1/1
No AL_PA value is specified. This will clear all AL_PA CRC counts on port 1. Do you want to continue? (yes, y, no, n): [no] y
Please wait ...
All alpa CRC counts are cleared on port 1.
```

In 3.1.0, 4.1.0, and later versions, you can use the `portStatsClear` command to clear AL_PA-based CRC error counters for all the ports in the same group.

Monitoring end-to-end performance

End-to-end performance monitoring counts the number of words and CRC errors in Fibre Channel frames for a specified Source ID (SID) and Destination ID (DID) pair. An end-to-end performance monitor includes these counts:

- RX_COUNT (words in frames received at the port)
- TX_COUNT (words in frames transmitted from the port)
- CRC_COUNT (frames with CRC errors received at or transmitted from the port)

To enable end-to-end performance monitoring, you must configure an end-to-end monitor on a port, specifying the SID-DID pair (in hexadecimal). The monitor counts only those frames with matching SID and DID.

Each SID or DID has the following three fields.

- Domain ID (DD)
- Area ID (AA)
- AL_PA (PP)

For example, the SID 0x118a0f denotes DD 0x11, AA 0x8a, and AL_PA 0x0f.

You can monitor end-to-end performance using the `perfMonitorShow` command, as described in “Displaying monitor counters” on page 357. You can clear end-to-end counters using the `perfMonitorClear` command, as described in “Clearing monitor counters” on page 361.
**NOTE:** For end-to-end monitors, CRC counters are not displayed on the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, 4/256 SAN Director, and DC Director switches.

### Adding end-to-end monitors

An end-to-end monitor counts the following items for a port: number of words received, number of words transmitted, and number of CRC errors detected in frames.

4/8 SAN Switch and 4/16 SAN Switch models allow up to eight end-to-end monitors.

The SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, and 4/256 SAN Director models allow up to 256 end-to-end monitors shared by all ports in the same ASIC chip. The DC Director allows up to 1024 end-to-end monitors. (The number of interswitch links configured on the switch affects the amount of resources available for end-to-end monitors.)

The FC4-48 blade allows end-to-end monitors on all 48 ports.

For the FC4-16IP blade, end-to-end monitors are supported on the FC ports (ports 0 through 7), but not on the GbE ports.

You cannot add end-to-end monitors to interswitch links. Identical end-to-end monitors cannot be added to the same port. Two end-to-end monitors are considered identical if they have the same SID and DID values after applying the end-to-end mask.

The monitor count is qualified using either of the following conditions:

- For frames received at the port with the end-to-end monitor installed, the frame SID is the same as “SourceID” and the frame DID is the same as “DestID”. The RX_COUNT and CRC_COUNT are updated accordingly.

- For frames transmitted from the port with the end-to-end monitor installed, the frame DID is the same as “SourceID” and the frame SID is the same as “DestID”. The TX_COUNT and CRC_COUNT are updated accordingly.

**NOTE:** The relationship between the area ID for a port and the port number depends on the PID format used by the fabric. See “Configuring the PID Format” on page 489 for more information.

Figure 27 shows two devices:

- Host A is connected to domain 5 (0x05), switch area ID 18 (0x12), AL_PA 0x00 on Switch X.
- Dev B is a storage device connected to domain 17 (0x11), switch area ID 30 (0x1e), AL_PA 0xef on Switch Y.

**Figure 27** Setting end-to-end monitors on a port

**NOTE:** End-to-end performance monitoring looks at traffic on the receiving port respective to the SID only. In Figure 27, if you add a monitor to slot 2, port 2 on Switch x, specifying Dev B as the SID and Host A as the DID, no counters (except CRC) will be incremented.
Monitoring the traffic from Host A to Dev B:
Add Monitor 0 to slot 2, port 2 on Switch x, specifying 0x051200 as the SID and 0x111eef as the DID, as shown in the following example:

```
switch:admin> perfadddeemonitor 2/2, "0x051200" "0x111eef"
End-to-End monitor number 0 added.
```

Monitor 0 counts the frames that have an SID of 0x051200 and a DID of 0x111eef. For monitor 0, RX_COUNT is the number of words from Host A to Dev B, TX_COUNT is the number of words from Dev B to Host A, and CRC_COUNT is the number of frames in both directions with CRC errors.

Monitoring the traffic from Dev B to Host A:
Add Monitor 1 to slot 2, port 14 on Switch y, specifying 0x111eef as the SID and 0x051200 as the DID, as shown in the following example.

```
switch:admin> perfadddeemonitor 2/14, "0x111eef" "0x051200"
End-to-End monitor number 1 added.
```

Monitor 1 counts the frames that have an SID of 0x111eef and a DID of 0x051200. For monitor 1, RX_COUNT is the number of words from Dev B to Host A, TX_COUNT is the number of words from Host A to Dev B, and CRC_COUNT is the number of frames in both directions with CRC errors.

Figure 28 shows several switches and the correct ports on which to add performance monitors for a specified SID-DID pair.

![Figure 28 Proper placement of end-to-end performance monitors](image)

**Setting a mask for end-to-end monitors**

End-to-end monitors count the number of words in Fibre Channel frames that match a specific SID/DID pair. If you want to match only part of the SID or DID, you can set a mask on the port to compare only certain parts of the SID or DID. By default, the frame must match the entire SID and DID to trigger the monitor. By setting a mask, you can choose to have the frame match only one or two of the three fields (Domain ID, Area ID, and AL_PA) to trigger the monitor.

**NOTE:** Only one mask per port can be set. When you set a mask, all existing end-to-end monitors are deleted.

You can specify a mask using the `perfSetPortEEMask` command in the form dd:aa:pp, where dd is the Domain ID mask, aa is the area ID mask, and pp is the AL_PA mask. The values for dd, aa, and pp are either ff (the field must match) or 00 (the field is ignored). The default EE mask value is ff:ff:ff. The `perfSetPortEEMask` command sets the mask for all end-to-end monitors of a port. If any end-to-end monitors are programmed on a port when the `perfSetPortEEMask` command is issued, then a message displays similar to the following example:

```
switch:admin> perfsetporteemask 1/2, "00:ff:ff"
EE monitors are currently programmed on this port. Changing EE mask for this port will cause ALL EE monitors on this port to be deleted.
Do you want to continue? (yes, y, no, n): [no] y
```

EE mask on port <port-number> is set and EE monitors were deletedThe `perfSetPortEEMask` command sets a mask for the Domain ID, Area ID, and
AL_PA of the SIDs and DIDs for frames transmitted from and received by the port.

**Figure 29** shows the mask positions in the command. A mask (“ff”) is set on slot 1, port 2 to compare the AL_PA fields on the SID and DID in all frames (transmitted and received) on port 2. The frame SID and DID must match only the AL_PA portion of the specified SID-DID pair. Each port can have only one EE mask. The mask is applied to all end-to-end monitors on the port. Individual masks for each monitor on the port cannot be specified.

![perfsetporteemask 1/2, "00:ff:ff" "00:ff:ff" "00:ff:ff" "00:ff:ff"](image)

**Figure 29** Mask positions for end-to-end monitors

On FC4-48 port blades, the upper 32 ports can be addressed only when the area ID and the AL_PA are used together. For usability concerns, the area ID and the AL_PA cannot be masked separately for any ports on FC4-48 port blades.

End-to-end masks are not supported on the DC Director.

**Deleting end-to-end monitors**

To delete an end-to-end monitor:

1. Enter the `perfShowEEMonitor` command to list the valid monitor numbers for a port.
2. Enter the `perfDelEEMonitor` command to delete a specific monitor.

   If you do not specify which monitor number to delete, you are asked if you want to delete all entries.

The following example displays the end-to-end monitors on port 0 using the `perfShowEEMonitor` command (the monitor numbers are listed in the KEY column) and deletes monitor number 2 on port 0 using the `perfDelEEMonitor` command:

```
switch:admin> perfshoweemonitor 0
There are 4 end-to-end monitor(s) defined on port 0.

KEY     SID     DID     OWNER_APP       TX_COUNT            RX_COUNT
OWNER_IP_ADDR
---------------------------------------------------------------------------
0 0x000024 0x000016  WEB_TOOLS   0x0000000000000000  0x0000000000000000 10.106.7.179
1 0x000022 0x000033  WEB_TOOLS   0x0000000000000000  0x0000000000000000 10.106.7.179
2 0x000123 0x000789  WEB_TOOLS   0x0000000000000000  0x0000000000000000 10.106.7.179
3 0x001212 0x003434  WEB_TOOLS   0x0000000000000000  0x0000000000000000 10.106.7.179
switch:admin> perfdeleemonitor 0, 2
End-to-End monitor number 2 deleted
switch:admin>
```
Monitoring filter-based performance

Filter-based performance monitoring counts the number of times a frame with a particular pattern is transmitted by a port. Filter-based monitoring is achieved by configuring a filter for a particular purpose. The filter can be a standard filter (for example, a SCSI read command filter that counts the number of SCSI read commands that have been transmitted by the port) or a user-defined filter customized for your particular use.

For the 4/8 SAN Switch and 4/16 SAN Switch models, the maximum number of filters is 8 per port, in any combination of standard filters and user-defined filters.

For the SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, and DC Director models, the maximum number of filters is 12 per port, in any combination of standard filters and user-defined filters.

For the 4/256 SAN Director models, the maximum number of filters is 12 per port, in any combination of standard filters and user-defined filters, except for the FC4-48 port blade. For the FC4-48 port blade:

- The lower 16 ports (ports 0 through 15) have a maximum of 12 filter monitors per port, and 15 offsets per port for used defined monitors.
- The middle 16 port (ports 16 through 31) have a maximum of 6 filter monitors per port, and 11 offsets per port for used defined monitors.
- The upper 16 ports (ports 32 through 47) do not support filter monitors.

The actual number of filters that can be configured on a port depends on the complexity of the filters. For trunked ports, the filter is configured on the trunk master.

You can monitor filter-based performance using the `perfMonitorShow` command, as described in “Displaying monitor counters” on page 357. You can clear filter-based counters using the `perfMonitorClear` command, as described in “Clearing monitor counters” on page 361.

Adding standard filter-based monitors

Table 78 lists the commands for adding standard filter-based monitors to a port.

**Table 78  Commands to add filter-based monitors**

<table>
<thead>
<tr>
<th>Telnet command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>perfAddReadMonitor</code></td>
<td>Count the number of SCSI Read commands</td>
</tr>
<tr>
<td><code>perfAddWriteMonitor</code></td>
<td>Count the number of SCSI Write commands</td>
</tr>
<tr>
<td><code>perfAddRwMonitor</code></td>
<td>Count the number of SCSI Read and Write commands</td>
</tr>
<tr>
<td><code>perfAddScsiMonitor</code></td>
<td>Count the number of SCSI traffic frames</td>
</tr>
<tr>
<td><code>perfAddIpMonitor</code></td>
<td>Count the number of IP traffic frames</td>
</tr>
</tbody>
</table>

You cannot add identical filter monitors to the same port. Two filter monitors are considered to be identical when they have the same values for the following items:

- Filter monitor type
- Owner (telnet, Web Tools, etc.)
- Alias

The following example adds filter-based monitors to slot 1, port 2 and displays the results:

```bash
switch:admin> perfaddreadmonitor 1/2
SCSI Read filter monitor #0 added
switch:admin> perfaddwritemonitor 1/2
SCSI Write filter monitor #1 added
switch:admin> perfaddrwmonitor 1/2
SCSI Read/Write filter monitor #2 added
```
switch:admin> perfaddscsimonitor 1/2
SCSI traffic frame monitor #3 added
switch:admin> perfaddipmonitor 1/2
IP traffic frame monitor #4 added
switch:admin> perfmonitorshow --class FLT 1/2
There are 5 filter-based monitors defined on port 2.

<table>
<thead>
<tr>
<th>KEY</th>
<th>ALIAS</th>
<th>OWNER_APP</th>
<th>FRAME_COUNT</th>
<th>OWNER_IP_ADDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SCSI Read</td>
<td>TELNET</td>
<td>0x0000000000000000</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>SCSI Write</td>
<td>TELNET</td>
<td>0x0000000000000000</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>SCSI R/W</td>
<td>TELNET</td>
<td>0x0000000000000000</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>SCSI Frame</td>
<td>TELNET</td>
<td>0x0000000000000000</td>
<td>N/A</td>
</tr>
<tr>
<td>4</td>
<td>IP Frame</td>
<td>TELNET</td>
<td>0x0000000000000000</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Adding custom filter-based monitors

In addition to the standard filters—read, write, read/write, SCSI frame and IP frame—you can create custom filters to gather statistics that fit your needs.

To define a custom filter, use the `perfAddUserMonitor` command. With this command, you must specify a series of offsets, masks, and values. For all transmitted frames, the switch performs these tasks:

- Locates the byte found in the frame at the specified offset.
- Applies the mask to the byte found in the frame.
- Compares the value with the given values in the `perfAddUserMonitor` command.
- Increments the filter counter if a match is found.

To illustrate, if you were to enter:

```
perfaddusermonitor 30 "4, 0xff, 0x06; 6, 0xff, 0x02; 7, 0xff, 0xd4"
```

The operation would be successful because offset 4 is a canned monitor and has a resource already reserved for it. Offsets 6 and 7 would exhaust all unique filter monitor resources on port 30. Therefore, any additional filter monitors created on port 30 would have to be canned filter monitors.

- SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, 4/256 SAN Director, and DC Director models
  Up to 15 different offsets per port (14 offsets when FICON Management Server mode, or fmsmode, is enabled).

- 4/8 SAN Switch, 4/16 SAN Switch and Brocade 4Gb SAN Switch for HP p-Class BladeSystem models
  Up to 7 different offsets per port (6 offsets when fmsmode is enabled).

You can specify up to four values to compare against each offset. If more than one offset is required to properly define a filter, the bytes found at each offset must match one of the given values for the filter to increment its counter. If one or more of the given offsets does not match any of the given values, the counter does not increment. The value of the offset must be between 0 and 63, in decimal format. Byte 0 indicates the first byte of the Start of Frame (SOF), byte 4 is the first byte of the frame header, and byte 28 is the first byte of the payload. Thus only the SOF, frame header, and first 36 bytes of payload can be selected as part of a filter definition. Offset 0 is a special case, which can be used to monitor the first 4 bytes of the...
frame (SOF). When the offset is set to 0, the values 0–7 that are checked against that offset are predefined as shown in Table 79.

Table 79  Predefined values at offset 0

<table>
<thead>
<tr>
<th>Value</th>
<th>SOFi</th>
<th>Value</th>
<th>SOFi</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SOFi4</td>
<td>4</td>
<td>SOFi2</td>
</tr>
<tr>
<td>1</td>
<td>SOFi1</td>
<td>5</td>
<td>SOFi2</td>
</tr>
<tr>
<td>2</td>
<td>SOFi3</td>
<td>6</td>
<td>SOFi3</td>
</tr>
<tr>
<td>3</td>
<td>SOFi3</td>
<td>7</td>
<td>SOFi3</td>
</tr>
</tbody>
</table>

If the switch does not have enough resources to create a given filter, then other filters might have to be deleted to free resources.

The following example adds filter-based monitors:

```
switch:admin> perfaddusermonitor 4/2, "12, 0xff, 0x05, 0x08; 9, 0xff, 0x02" "FCP/IP"
User monitor #5 added

switch:admin> perfaddusermonitor 1/2, "0, 0xff, 6"
User Monitor #6 added
```

Two filter-based monitors are added. The first monitor (#5) counts all FCP and IP frames transmitted from domain 0x02 for slot 4, port 2. The FCP and IP protocols are selected by monitoring offset 1 2, mask 0xff and matching values of 0x05 or 0x08. Domain 2 is selected by monitoring offset 9, mask 0xff, and matching a value of 0x02. The monitor counter is incremented for all outgoing frames from port 2 where byte 9 is 0x02 and byte 12 is 0x05 or 0x08.

The second monitor (#6) is for SOFi3 on slot 1, port 2.

### Deleting filter-based monitors

To delete a filter-based monitor:

1. Enter the `perfDelFilterMonitor` command to delete a specific monitor.

   If you do not specify which monitor number to delete, you are asked if you want to delete all entries.

The following example deletes monitor number 1 on slot 1, port 4 using the `perfDelFilterMonitor` command:

```
switch:admin> perfdelfiltermonitor 1/4, 1
The specified filter-based monitor is deleted.
```

### Monitoring ISL performance

ISL monitoring is set up on E_Ports automatically in release 4.4.0 and later.

An ISL monitor measures traffic to all reachable destination domains for an ISL, showing which destination domain is consuming the most traffic. If there are more than 16 domains, the monitor samples traffic and extrapolates the measurement.

EE monitors on E_Ports are deleted when they become part of an ISL.

ISL monitors are deleted when Top Talker is installed and are restored when Top Talker is deleted. (See “Identifying top bandwidth users (Top Talkers)” for information about Top Talker monitors.)

You can monitor ISL performance using the `perfMonitorShow` command, as described in “Displaying monitor counters.” You can clear ISL counters using the `perfMonitorClear` command, as described in “Clearing monitor counters” on page 361.

ISL monitoring is not supported on the DC Director.
Identifying top bandwidth users (Top Talkers)

Top Talker monitors determine the flows (SID/DID pairs) that are the major users of bandwidth (after initial stabilization). Top Talker monitors measure bandwidth usage data in real-time and relative to the port on which the monitor is installed.

**NOTE:** *Initial stabilization* is the time taken by a flow to reach the maximum bandwidth. This time varies depending on the number of flows in the fabric and other factors. The incubation period can be up to 14 seconds in the DC Director and up to 82 seconds in the SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, and 4/256 SAN Director.

Top Talker can be installed only on switches that run Fabric OS 6.0.0 or later. Top Talker monitors are not supported on the 4/8 SAN Switch, 4/16 SAN Switch.

Applications can use the Top Talker data to do the following:

- Re-route the traffic through different ports that are less busy, so as not to overload a given port.
- Alert you of the top-talking flows on a port if the total traffic on the port exceeds the acceptable bandwidth consumption.

You can use Top Talkers to identify the SID/DID pairs that consume the most bandwidth and can then configure them with certain Quality of Service (QoS) attributes so they get proper priority. See “Optimizing fabric behavior” on page 333 for information on QoS.

The Top Talker monitor is based on SID/DID and not WWNs. Once Top Talker is installed on a port, it remains installed across power cycles.

Top Talker supports two modes: port mode and fabric mode.

- **Port mode Top Talker**
  A Top Talker monitor can be installed on an F_Port to measure the traffic originating from the F_Port and flowing to different destinations.

- **Fabric mode Top Talker**
  In fabric mode, Top Talker monitors are installed on all E_Ports in the fabric and measure the data rate of all the possible flows in the fabric (ingress E_Port traffic only). In fabric mode, Top Talker monitors can determine the top \( n \) bandwidth users on a given switch.

You can install Top Talker monitors either in port mode or fabric mode, but not both.

**How do Top Talker monitors differ from end-to-end monitors?** End-to-end monitors provide counter statistics for traffic flowing between a given SID-DID pair. Top Talker monitors identify all possible SID-DID flow combinations that are possible on a given port and provides a sorted output of the top talking flows. Also, if the number of flows exceeds the hardware resources, existing end-to-end monitors fail to get real time data for all of them; however, Top Talker monitors can monitor all flows for a given port (E_Port or F_Port).

**Admin Domain considerations:** Top Talker monitors are always installed in AD255.

**NPIV considerations:** Top Talker takes NPIV devices into consideration when calculating the top talking flows.
Using Top Talker monitors in port mode

Use the perfttmon command to add, delete, and display Top Talker monitors. Refer to the Fabric OS Command Reference for details about the perfttmon command.

To add a Top Talker monitor on an F_Port:

1. Connect to the switch and log in as admin.
2. Enter the perfttmon --add command.
   
   perfttmon --add [egress | ingress] [slotnumber/]port
   
   where:
   slotnumber For director-class switches only (4/256 SAN Director and DC Director), the slot number.
   port The port number.

   For example, to monitor the incoming traffic on port 7:
   perfttmon --add ingress 7

   To monitor the outgoing traffic on slot 2, port 4 on the 4/256 SAN Director or DC Director:
   perfttmon --add egress 2/4

To delete a Top Talker monitor on an F_Port:

1. Connect to the switch and log in as admin.
2. Enter the perfttmon --delete command.
   
   perfttmon --delete [slotnumber/]port
   
   where:
   slotnumber For director-class switches only (4/256 SAN Director and DC Director), the slot number.
   port The port number.

   For example, to delete the monitor on port 7:
   perfttmon --delete 7

   To delete the monitor on slot 2, port 4 on the 4/256 SAN Director or DC Director:
   perfttmon --delete 2/4

To display the top $n$ bandwidth-using flows on an F_Port:

1. Connect to the switch and log in as admin.
2. Enter the perfttmon --show command.
   
   perfttmon --show [slotnumber/]port [n] [wwn | pid]
   
   where:
   slotnumber For director-class switches only (4/256 SAN Director and DC Director), the slot number.
   port The port number.
   n The number of top talking flows to display, between 1 and 32.
   wwn | pid The format of the output. The default is wwn.

   The output is sorted based on the data rate of each flow. If you do not specify the number of flows to display, then the command displays the top 8 flows or the total number of flows, whichever is less. The command can display a maximum of 32 flows.
For example, to display the top 5 flows on port 7 in WWN (default) format:

```
perfttmon --show 7 5
```

To display the top flows on slot 2, port 4 on the 4/256 SAN Director or DC Director in PID format:

```
perfttmon --show 2/4 pid
```

```
switch:admin> perfttmon --show 2/4 pid

========================================
<table>
<thead>
<tr>
<th>Src_PID</th>
<th>Dst_PID</th>
<th>MB/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xa90800</td>
<td>0xa05200</td>
<td>6.926</td>
</tr>
<tr>
<td>0xa90800</td>
<td>0xa908ef</td>
<td>6.872</td>
</tr>
</tbody>
</table>
```

**Using Top Talker monitors in fabric mode**

When fabric mode is enabled, you can no longer install Top Talker monitors on an F_Port unless you delete fabric mode.

Use the `perfttmon` command to add, delete, and display Top Talker monitors. Refer to the *Fabric OS Command Reference* for details about the `perfttmon` command.

To add Top Talker monitors on all switches in the fabric:

1. Connect to the switch and log in as admin.
2. Enter the `perfttmon --add fabricmode` command.

```
perfttmon --add fabricmode
```

Top Talker monitors are added to all E_Ports in the fabric and fabric mode is enabled. Any Top Talker monitors that were already installed on F_Ports are automatically uninstalled.

If a new switch joins the fabric, you must run the `perfttmon --add fabricmode` command on the new switch. The Top Talker configuration information is not automatically propagated to the new switch.

To delete the fabric mode Top Talker monitors:

1. Connect to the switch and log in as admin.
2. Enter the `perfttmon --delete fabricmode` command.

```
perfttmon --delete fabricmode
```

All Top Talker monitors are deleted.

To display top talking flows on the switch for a given Domain ID:

1. Connect to the switch and log in as admin.
2. Enter the `perfttmon --show dom` command.

```
perfttmon --show dom domainid [n] [wwn | pid]
```

where:

- `domainid` The Domain ID of the switch.
- `n` The number of top talking flows to display, between 1 and 32.
- `wwn | pid` The format of the output. The default is `wwn`.

Fabric mode must be enabled for this option.

The output is sorted based on the data rate of each flow. If you do not specify the number of flows to display, then the command displays the top 8 flows or the total number of flows, whichever is less. The command can display a maximum of 32 flows.

For example, to display the top 5 flows on for domain 1 in WWN (default) format:

```
perfttmon --show dom 1 5
```
To display the top flows on domain 2 in PID format:

```
perfttmon --show dom 2 pid
```

```
switch:admin> perfttmon --show dom 2 pid
```

```
+---------------------------------------
<table>
<thead>
<tr>
<th>Src_PID</th>
<th>Dst_PID</th>
<th>MB/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>0xa908ef</td>
<td>0xa05200</td>
<td>6.926</td>
</tr>
<tr>
<td>0xa05200</td>
<td>0xa908ef</td>
<td>6.872</td>
</tr>
<tr>
<td>0xa905ef</td>
<td>0xa05200</td>
<td>6.830</td>
</tr>
<tr>
<td>0xa909d5</td>
<td>0xa05200</td>
<td>6.772</td>
</tr>
</tbody>
</table>
```

Limitations of Top Talker monitors

- Top Talker monitors cannot detect transient surges in traffic through a given flow.
- You cannot install a Top Talker monitor on a mirrored port.
- Top Talker can monitor only 10,000 flows at a time.
- Top Talker is not supported on VE_Ports, EX_Ports, and VEX_Ports.

Monitoring trunks

For trunked ISLs on Fabric OS 4.x or later switches, monitoring is set only on the master ISL, which communicates with the associated slave ISLs. Note the following:

- For Fabric OS 3.x switches, monitoring can be set on slave ISLs.
- End-to-end monitors are not supported for ISLs.
- 4/8 SAN Switch, 4/16 SAN Switch models support 8 filter-based monitors for trunks.
- The SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, 4/256 SAN Director and DC Director switches support 12 filter-based monitors for trunks.

Displaying monitor counters

Use the `perfMonitorShow` command to display the monitors on a specified port. For end-to-end counters, you can display either the cumulative count of the traffic detected by the monitors or a snapshot of the traffic at specified intervals.

**NOTE:**

4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 Multi-protocol Router, 4/256 SAN Director, and DC Director output does not include CRC counts.

```
The command format is:

```
perfmonitorshow --class monitor_class [slotnumber/]portnumber [interval]
```

**monitor_class** The monitor class, which can be one of EE (end-to-end), FLT (filter-based), or ISL (inter-switch link). The --class monitor_class operand is required.
**slotnumber** Specifies the slot number for a 4/256 SAN Director director. For all other switches, this operand is not required. The slot number must be followed by a slash (/) and the port number, so that each port is represented by both slot number (1 through 4 or 7 through 10) and port number (0 through 15).

The Directors have a total of 10 slots. Slot numbers 5 and 6 are control processor blades; slots 1 through 4 and 7 through 10 are port blades. For 16-port blades, there are 16 ports, counted from the bottom, numbered 0 to 15. For 32-port blades, there are 32 ports numbered 0 to 31.

**portnumber** Specifies a port number. Valid values for port number vary, depending on the switch type. This operand is required.

**interval** Specifies an interval in seconds. The interval must be greater than or equal to five seconds. For end-to-end monitoring, the Tx and Rx counts are measured in bytes. This operand is optional.
The following example displays an end-to-end monitor on a port at 6-second intervals:

```
switch:admin> perfMonitorShow --class EE 4/5 6
```

```
 perfmonitorshow 53, 6: Tx/Rx are # of bytes and crc is # of crc errors
```

```
0            1            2            3            4
------------- ------------- ------------- ------------- -------------
  crc   Tx   Rx   crc   Tx   Rx   crc   Tx   Rx   crc   Tx   Rx
------------- ------------- ------------- ------------- -------------
0    0     0   0    0    0  0    0     0   0    0    0   0     0   0
0  53m  4.9m  0  53m 4.9m  0  53m  4.9m  0  53m  4.9m  0  53m  0
0  53m  4.4m  0  53m 4.4m  0  53m  4.4m  0  53m  4.4m  0  53m  0
0  53m  4.8m  0  53m 4.8m  0  53m  4.8m  0  53m  4.8m  0  53m  0
0  53m  4.6m  0  53m 4.6m  0  53m  4.6m  0  53m  4.6m  0  53m  0
0  53m  5.0m  0  53m 5.0m  0  53m  5.0m  0  53m  5.0m  0  53m  0
0  53m  4.8m  0  53m 4.8m  0  53m  4.8m  0  53m  4.8m  0  53m  0
0  53m  4.5m  0  53m 4.5m  0  53m  4.5m  0  53m  4.5m  0  53m  0
0  52m  4.5m  0  52m 4.5m  0  52m  4.5m  0  52m  4.5m  0  52m  0
0  52m  5.0m  0  52m 5.0m  0  52m  5.0m  0  52m  5.0m  0  52m  0
0  52m  4.5m  0  52m 4.5m  0  52m  4.5m  0  52m  4.5m  0  52m  0
0  52m  4.6m  0  52m 4.6m  0  52m  4.6m  0  52m  4.6m  0  52m  0
```

The following example displays EE monitors on a port:

```
switch:admin> perfMonitorShow --class EE 4/5
```

```
There are 7 end-to-end monitor(s) defined on port 53.
```

```
KEY     SID     DID     OWNER_APP TX_COUNT          RX_COUNT
CRC_COUNT OWNER_IP_ADDR
```

```
-------------------------------------------------------------------------
--------------------------------
0  0x58e0f  0x1182ef   TELNET 0x0000000000000000  0x0000000000000000  N/A
0x0000000000000000 0x0000000000000000
0  0x21300  0x21dda    TELNET 0x00000004d0ba9915 0x0000000067229e65  N/A
0x0000000000000000 0x0000000000000000
1  0x21300  0x21ddc    TELNET 0x00000004d0baa754 0x0000000067229e65  N/A
0x0000000000000000 0x0000000000000000
2  0x21300  0x21de0    TELNET 0x000000004d0bab3a5 0x0000000067229e87  N/A
0x0000000000000000 0x0000000000000000
3  0x21300  0x21de1    TELNET 0x000000004d0bac1e4 0x0000000067229e87  N/A
0x0000000000000000 0x0000000000000000
4  0x21300  0x21de2    TELNET 0x000000004d0bad086 0x0000000067229e87  N/A
0x0000000000000000 0x0000000000000000
5  0x11000  0x21fd6 WEB_TOOLS 0x000000004d0bad54 0x0000000067229e87 192.168.169.40
0x0000000000000000 0x0000000000000000
6  0x11000  0x21fe0 WEB_TOOLS 0x000000004d0baed41 0x0000000067229e98 192.168.169.40
0x0000000000000000 0x0000000000000000
```
The following example displays a filter-based monitor on a port at 6-second intervals:

```
switch:admin> perfMonitorShow --class FLT 2/5 6
```

```
0  1  2  3  4  5  6
#Frames #Frames #Frames #Frames #Frames #Frames #Frames
---------------------------------------------------------------------
0       0       0       0       0       0       0
26k     187     681     682     682     494     187
26k     177     711     710     710     534     176
26k     184     734     734     734     550     184
26k     182     649     649     649     467     182
26k     188     754     755     755     567     184
26k     183     716     716     717     534     183
26k     167     657     656     655     488     167
26k     179     749     749     749     570     179
26k     164     752     752     752     588     164
26k     190     700     700     700     510     190
26k     181     701     701     701     520     181
26k     200     750     750     751     550     201
26k     180     692     692     691     512     179
26k     179     696     696     696     517     179
26k     187     720     720     720     533     187
26k     200     722     722     722     522     200
26k     204     717     717     717     513     204
```

The following example displays filter monitor information on a port:

```
switch:admin> perfMonitorShow --class FLT 2/5
There are 7 filter-based monitors defined on port 21.

KEY   ALIAS   OWNER_APP     FRAME_COUNT         OWNER_IP_ADDR
---------------------------------------------------------------------
0      SCSI_Frame  TELNET   0x000000000002c2229     N/A
1      SCSI_WR     TELNET   0x000000000000464a     N/A
2      SCSI_RW     TELNET   0x000000000000fd8c     N/A
3      SCSI_RW     WEB_TOOLS 0x0000000000000464a 192.168.169.40
4      SCSI_RW     WEB_TOOLS 0x00000000000004f0e 192.168.169.190
5      SCSI_RD     WEB_TOOLS 0x0000000000002208 192.168.169.40
6      SCSI_WR     WEB_TOOLS 0x00000000000033a 192.168.169.40
```

The following example displays ISL monitor information on a port:

```
switch:admin> perfMonitorShow --class ISL 1/1
Total transmit count for this ISL: 1462326
Number of destination domains monitored: 3
Number of ports in this ISL: 2
Domain 97: 110379    Domain 98: 13965
Domain 99: 1337982
```
Known display problem and workaround

When two shared ports on an FC4-48 blade are receiving traffic and the primary port goes offline, all the frames that are out for delivery for the primary port are dropped, but the counters show them as dropped on the secondary port that shares the same area. Error counters increment unexpectedly for the secondary port, but the secondary port is operating properly.

If this occurs, clear the counters on the secondary port after primary port goes offline.

Clearing monitor counters

Before you clear statistics counters, verify the valid monitor numbers on a specific port using the perfMonitorShow command, to make sure the correct monitor counters are cleared. To clear statistics counters for all or a specified monitor, use the perfMonitorClear command. After the command has been executed, the Telnet shell confirms that the counters on the monitor have been cleared.

The command format is:

```
perfmonitorclear --class monitor_class [slotnumber/]portnumber [monitorId]
```
NOTE: In Fabric OS 3.1.0 and 4.1.0 (or later) the `portStatsClear` command clears AL_PA-based CRC error counters for all the ports in the same group.

The following example clears statistics counters for an end-to-end monitor:
```
switch:admin> perfMonitorClear --class EE 1/2 5
End-to-End monitor number 5 counters are cleared
```
```
switch:admin> perfMonitorClear --class EE 1/2
This will clear ALL EE monitors' counters on port 2, continue? (yes, y, no, n): [no] y
```

The following example clears statistics counters for a filter-based monitor:
```
switch:admin> perfMonitorClear --class FLT 1/2 4
Filter-based monitor number 4 counters are cleared
```
```
switch:admin> perfMonitorClear --class FLT 1/2
This will clear ALL filter-based monitors' counters on port 2, continue? (yes, y, no, y): [no] y
```

The following example clears statistics counters for an ISL monitor:
```
switch:admin> perfMonitorClear --class ISL 1
This will clear ISL monitor on port 1, continue? (yes, y, no, n): [no] y
```
Saving and restoring monitor configurations

To save the current end-to-end and filter monitor configuration settings into nonvolatile memory, use the `perfCfgSave` command:

```
switch:admin> perfCfgSave
This will overwrite previously saved Performance Monitoring
settings in FLASH. Do you want to continue? (yes, y, no, n): [no] y
Please wait ...
Performance monitoring configuration saved in FLASH.
```

To restore a saved monitor configuration, use the `perfCfgRestore` command. For example, to restore the original performance monitor configuration after making several changes:

```
switch:admin> perfCfgRestore
This will overwrite current Performance Monitoring settings in RAM. Do you want to continue? (yes, y, no, n): [no] y
Please wait... Performance monitoring configuration restored from FLASH ROM.
```

To clear the previously saved performance monitoring configuration settings from nonvolatile memory, use the `perfCfgClear` command:

```
switch:admin> perfCfgClear
This will clear Performance Monitoring settings in FLASH. The RAM settings won’t change. Do you want to continue? (yes, y, no, n): [no] y
Please wait... Committing configuration...done.
Performance Monitoring configuration cleared from FLASH.
```

To prevent the switch configuration flash from running out of memory, the number of monitors saved to flash memory is limited as follows:

- The total number of EE monitors per port is limited to 16.
- The total number of filter monitors per port is limited to 16.
- The total number of monitors per switch is limited to 512.

When there are more than 512 monitors in the system, monitors are saved to flash memory in the following order:

- The EE monitors for each port (from 0 to MAX_PORT)
- The filter monitors for each port

EE monitors get preference saving to flash memory when the total number of monitors in a switch exceeds 512. If the total number of monitors per port or switch exceeds the limit, then you will receive an error message indicating the count has been exceeded and that some monitors have been discarded.

Collecting performance data

Data collected through Advanced Performance Monitoring is deleted when the switch is rebooted. Using the Fabric Manager software application version 4.4.0 or later, you can store performance data persistently. For details on this feature, see the Fabric Manager Administrator’s Guide.
18 Administering Extended Fabrics

This chapter provides information on implementing Extended Fabrics software.

Extended Fabrics licensing

To implement long distance dynamic (LD) and long distance static (LS) distance levels, you must first install the Extended Fabrics license. Use the `licenseShow` command to verify that the license is present on both switches used on both ends of the extended ISL.

Extended Fibre Channel over distance

Extended Fabrics software optimizes switch buffering to ensure the highest possible performance on inter-switch links (ISLs). When Extended Fabrics is installed on gateway switches, the ISLs (E_Ports) are configured with a large pool of buffer credits. The enhanced switch buffers help ensure that data transfer can occur at near-full bandwidth to efficiently utilize the connection over the extended links.

The Extended Fabrics feature extends the distance the ISLs can reach over a dark fiber or wave division multiplexing (WDM) connection. This is accomplished by providing enough buffer credits on each side of the link to compensate for latency introduced by the extended distance.

Distance levels for extended Inter-Switch Links (ISLs)

As the distance between switches and the link speed increases, additional buffer credits are required for the ports used for long distance connections. Distance levels define how these buffer credits are allocated and managed for extended ISLs. Buffer credits are managed from a common pool available to a group of ports on a switch. The buffer credit, can be changed for specific applications or operating environments, but must be in agreement among all switches to allow formation of the fabric.

Information about switch characteristics and capacity in terms of buffers per port group, port speed, and distances supported is in Table 81 on page 368. This table may be useful in choosing an appropriate distance level, and for estimating the impact an extended ISL may have on buffer availability and port performance.

Buffer-to-Buffer Credits

Buffer-to-buffer (BB) credit flow control is implemented to limit the amount of data a port may send based on the number and size of the frames sent from that port. Buffer credits represent finite physical port memory. Within a fabric, each port may have a different number of BB credits. Within a connection, each side may have a different number of BB credits. One buffer credit allows a device to send one payload up to 2112 bytes (2148 with headers). Assuming that each payload is 2112, you need one credit per 1 km of link length at 2 Gbps (smaller payloads require additional BB credits to maintain link utilization).

The final frame size must be a multiple of 4 bytes. If the data (payload) needs to segment, it will be padded with 1 to 3 “fill-bytes” to achieve an overall 4 byte frame alignment. The standard frame header size is 24 bytes. If applications require extensive control information, up to 64 additional bytes (for a total of an 88 byte header) can be included. Because the total frame size cannot exceed the maximum of 2,148 bytes, the additional header bytes will subtract from the data segment size by as much as 64 bytes (per frame). This is why the maximum data (payload) size is 2,112 (because [2,112 – 64] = 2,048, which is exactly 2K-bytes of data). The final frame, after it is constructed, is passed through the 8 byte to 10 byte conversion process.
Table 80 describes Fibre Channel data frames

<table>
<thead>
<tr>
<th>Description</th>
<th>Length</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start of frame</td>
<td>4 bytes</td>
<td>32 bits</td>
</tr>
<tr>
<td>Standard frame header</td>
<td>24 bytes</td>
<td>192 bits</td>
</tr>
<tr>
<td>Data (payload)</td>
<td>{0 - 2,112 bytes}</td>
<td>{0 - 16,896} bits</td>
</tr>
<tr>
<td>CRC</td>
<td>4 bytes</td>
<td>32 bits</td>
</tr>
<tr>
<td>End of frame</td>
<td>4 bytes</td>
<td>32 bits</td>
</tr>
<tr>
<td>Total (Nbr bits/frame)</td>
<td>{36 0 2,148} bytes</td>
<td>288 - 17,184 bits</td>
</tr>
</tbody>
</table>

The term byte used in Table 80 means 8 bits. The maximum fibre channel frame is 2,148 bytes.

You can allocate buffer credit using the `portCfgLongDistance` command, which allows you to allocate sufficient numbers of full-size frame buffers on a particular port or to support a long distance link up to 500 km. The port can only be used as an E_Port. Changes made by this command are persistent across switch reboots and power cycles.

Use the `portCfgLongDistance --distance_level` command to select one of the following four options for buffer credit allocation:

- Level 0 static mode (L0) - L0 is the normal mode for a port. An extended ISL port competes with other ports for buffers. No buffer credits are reserved for extended ISLs.
- Level E static mode (LE) - LE reserves a static number of buffer credits that supports distances up to 10 km. The number reserved depends on the port speed. The baseline for the calculation is one credit per km at 2 Gbps. This yields the following values for 10 km:
  - 5 credits per port at 1 Gbps.
  - 10 credits per port at 2 Gbps.
  - 20 credits per port at 4 Gbps.
  - 40 credits per port at 8 Gbps.
- Dynamic Mode (LD) - LD calculates buffer credits based on the distance measured during port initialization. An upper limit is placed on the calculation by providing a desired distance value. When the measured distance is more than desired distance, the desired distance is used in the calculation. This is a mechanism for controlling the number of reserved buffer credits ensuring buffer availability for other ports in the same group.
- Static long distance mode (LS) - LS calculates a static number of buffer credits based on a desired distance value.

For both LD and LS distance levels, you can use the following formula to get an approximation of the calculated number of buffer credits.
FC switch port Buffer Credit requirements for long distance calculations

You can calculate how many ports can be configured for long distance on all switch modules or ASICs except Bloom-based switches. For information on the port, speed and distance for Bloom-based ASICs, see Table 82. Following are the considerations for the calculation:

- Each user port reserves eight buffers when they are not online.
- Remaining buffers can be reserved by any port in the port group.
- When QoS is enabled and the port is online, an additional 14 buffers are allocated.
- Condor-based switches have a limitation of 255 buffers maximum, which can be allocated by a port; this limits the distance of ~500km at 1G.
- For LD, distance in km is the smaller of the distance measured during port initialization versus the desired distance value.
- For LS, distance in km is always the desired distance value.

Before you can calculate the buffer requirement, note the following Fibre Channel gigabit values reference definition:

- 1.0625 for 1 Gbps
- 2.125 for 2 Gbps
- 4.25 for 4 Gbps
- 8.5 for 8 Gbps

Determining how many ports can be configured for long distance

**NOTE:** The following formula is used to determine the number of buffer credits:

$$\text{buffer credits} = \left\lfloor \left( \text{distance in km} \times \text{data rate} \times 1000 \right) / 2112 \right\rfloor$$

1. Determine the distance in kilometers between switch-to-switch. For this example we will use 50km.
2. Determine the speed that you will use for the long distance connection. For this example, we will use 2 Gbps.
3. Use the following formula to get the reserved buffers for distance:

$$\text{Reserved Buffer for Distance} = (X \times \text{LinkSpeed} / 2) + 6$$

Where:

- $X$ = the distance determined in step 1.
- LinkSpeed = the speed of the link determined in step 2.
- 6 = the number of buffer credits reserved for Fabric Services, Multicast, and Broadcast traffic. This is a static number.

Based on the answers provided in steps 1 and 2, plug the numbers into the formula. The formula should read as follows:

$$\left(50\text{km} \times 2\text{ Gbps} / 2\right) + 6 = 56 \text{ buffers}$$

Below are additional examples using different speeds all base on a distance of 50km. The distances and speeds are variables which can change based on how your network is set up.

- If you have a distance of 50km at 1 Gbps then, $(50\text{km} \times 1\text{ Gbps} / 2) + 6 = 31 \text{ buffers}$
- If you have a distance of 50km at 2 Gbps then, $(50\text{km} \times 2\text{ Gbps} / 2) + 6 = 56 \text{ buffers}$
- If you have a distance of 50km at 4Gbps then, $(50\text{km} \times 4\text{ Gbps} / 2) + 6 = 106 \text{ buffers}$
- If you have a distance of 50km at 8 Gbps then, $(50\text{km} \times 8\text{ Gbps} / 2) + 6 = 206 \text{ buffers}$
**Example:** Consider the 4/16 SAN Switch, which has 16 ports and total buffers of 272

The maximum remaining number of buffer credits after each port is reserved is:

\[ 272 - (16 \times 8) = 144 \text{ buffers} \]

Where:

- \(16\) = the number of ports in a port group retrieved from Table 81.
- \(8\) = the number of reserved buffers
- \(272\) = a static number retrieved from Table 81.

If you allocate the entire 144 + 8 reserved buffers = 152 buffers to a single port; you can have one port 146km @ 2G or 292km @ 1G.

How many 50km ports you can configure?

If you have a distance of 50km at 1 Gbps then \(144 / (31 - 8) = 6\) ports.

**NOTE:** The 10 Gbps FC10-6 blade has two port groups of three ports each. For extended ISLs, all buffers available to a group are used to support one port at up to 120 km.

**Displaying the remaining buffers in a port group**

Issue the `portbuffershow` command to display all of the long distance buffer information for all the port groups of the switch. Use the following syntax:

```
portbuffershow [[slotnumber/]portnumber]
```

- `slotnumber` For bladed systems only, specifies the slot number of the port group to display, followed by a slash (/).
- `portnumber` Specifies the number of a port associated with the port group, relative to its slot for bladed systems. Use switchShow for a list of valid ports.

1. Connect to the switch and log in as admin.
2. Enter the `portbuffershow` command.

```
switch:admin> portbuffershow 1
```

<table>
<thead>
<tr>
<th>User Port</th>
<th>Type</th>
<th>Mode</th>
<th>Max/Resv Buffers</th>
<th>Buffer Needed Usage Buffers</th>
<th>Link Distance Buffers</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>4</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>11</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>16</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>17</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>18</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>20</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>21</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>22</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>23</td>
<td>U</td>
<td>-</td>
<td>8</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

```
switch:admin>
### Table 81 Switch, port speed, and distance with ASIC and buffers

<table>
<thead>
<tr>
<th>Switch blade model</th>
<th>ASIC</th>
<th>Total ports in a switch or blade</th>
<th>Total ports in a group</th>
<th>Reserved buffers for ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-Series 2Gb Switches</td>
<td>Bloom</td>
<td>8, 16 or 32</td>
<td>108/4</td>
<td>0</td>
</tr>
<tr>
<td>4/8 SAN Switch or 4/16 SAN Switch</td>
<td>Golden Eye</td>
<td>16</td>
<td>272/16</td>
<td>8</td>
</tr>
<tr>
<td>SAN Switch 4/32 and SAN Switch 4/328</td>
<td>Condor</td>
<td>32</td>
<td>1000/32</td>
<td>8</td>
</tr>
<tr>
<td>4/64 SAN Switch</td>
<td>Condor</td>
<td>64</td>
<td>712/16</td>
<td>8</td>
</tr>
<tr>
<td>400 Multi-protocol (MP) Router</td>
<td>Condor</td>
<td>16</td>
<td>441/8</td>
<td>8</td>
</tr>
<tr>
<td>FR4-18i</td>
<td>Condor</td>
<td>16</td>
<td>441/8</td>
<td>8</td>
</tr>
<tr>
<td>FC4-16iP</td>
<td>Condor</td>
<td>8</td>
<td>680/8</td>
<td>8</td>
</tr>
<tr>
<td>FC4-16</td>
<td>Condor</td>
<td>16</td>
<td>712/16</td>
<td>8</td>
</tr>
<tr>
<td>FC4-32</td>
<td>Condor</td>
<td>32</td>
<td>752/16</td>
<td>8</td>
</tr>
<tr>
<td>FC4-48</td>
<td>Condor</td>
<td>48</td>
<td>752/24</td>
<td>8</td>
</tr>
<tr>
<td>FC10-6</td>
<td>Egret and Condor</td>
<td>6</td>
<td>712/1</td>
<td>N/A</td>
</tr>
<tr>
<td>FC8-16</td>
<td>Condor2</td>
<td>16</td>
<td>1420/16</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1516/16</td>
<td></td>
</tr>
<tr>
<td>FC8-32</td>
<td>Condor2</td>
<td>32</td>
<td>1420/16</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1516/16</td>
<td></td>
</tr>
<tr>
<td>FC8-48</td>
<td>Condor2</td>
<td>48</td>
<td>1420/24</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1516/24</td>
<td></td>
</tr>
<tr>
<td>Brocade 4Gb SAN Switch for HP p-Class BladeSystem</td>
<td>Golden Eye</td>
<td>12</td>
<td>272/12</td>
<td>8</td>
</tr>
<tr>
<td>Brocade 4Gb SAN Switch for HP c-Class BladeSystem</td>
<td>Golden Eye</td>
<td>24</td>
<td>272/24</td>
<td>8</td>
</tr>
</tbody>
</table>

**NOTE:** Additional buffers are available with 4Gbps chassis for 8Gbps blades because of fewer buffers allocated for back-end port connections.
Fabric considerations

Because the number of buffer credits available for use within each port group is limited, configuring buffer credits for extended links may impact the performance of the other ports in the group used for core-to-edge connections. Balance the number of long-distance ISL connections and core-to-edge ISL connections within a switch. Configuring long-distance ISLs between core and edge switches is possible, but is not a recommended practice.

With the exception of older switches and blades that use the Bloom ASIC, all switch ports provide protection against buffer depletion through buffer limiting. A buffer-limited port reserves a minimum of eight buffer credits, allowing the port to continue to operate rather than being disabled due to a lack of buffers. The 8 buffer minimum allows 4 Gbps speeds over distances within most data centers.

Buffer-limited operation is supported for the L0 and LD extended ISL modes only, and is persistent across reboots, switch disabling and enabling, and port disabling and enabling.

Long distance link initialization activation

VC translation link initialization (vc_translation_link_init), a parameter of the portCfgLongDistance command, is enabled by default for long-distance links. To avoid inconsistency in the fabric, make sure that this parameter is enabled on both ends of the link by entering the portCfgLongDistance --vc_translation_link_init command. Specify 1 to activate long distance link initialization sequence; specify 0 to deactivate this mode. When the command is run without specifying a value, 1 is assigned automatically for the long-distance link in VC_R_RDY flow control; otherwise, 0 is assigned. For a long-distance link not configured for ISL R_RDY mode, this parameter must be set to 1; otherwise, it must be reset to 0.

Extended Fabrics device limitations

Extended Fabrics is normally not implemented on the following devices.

- The 400 Multi-protocol (MP) Router and the FR4-18i blade integrate two Gigabit Ethernet ports and sixteen FC ports. The two Gigabit Ethernet ports provide SAN extension over IP networks using FCIP.
- The FC4-16IP blade integrates eight Gigabit Ethernet ports and eight FC ports. It is used to implement the iSCSI Gateway Service. The Gigabit Ethernet ports are used to connect iSCSI initiators, and the FC ports are used to connect to any device.

Configuring an extended ISL

Before configuring an extended ISL, ensure that the following conditions are met:

- Be sure that the ports on both ends of the ISL are operating at the same port speed, and can be configured at the same distance level without compromising local switch performance.
- Use only qualified Brocade SFPs.

**NOTE:** A long-distance link also can be configured to be part of a trunk group. Two or more long-distance links in a port group form a trunk group when they are configured for the same speed, the same distance level, and their link distances are nearly equal. For information on trunking concepts and configurations, refer to “Administering ISL Trunking” on page 377.

- Use only qualified HP SFPs.
- For fabrics that contain B-Series 2Gb switches, contact HP support for details on which parameters to set.
- For Fabric OS 3.x or 4.x, contact HP for details on which parameters to set.

1. Connect to the switch and log in as admin.
2. Enter the switchDisable command.
3. Enter the configure command to set the switch fabric-wide configurations. You can set the following fabric-wide settings:

(* = multiplication symbol)

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Default</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Number</td>
<td>1</td>
<td>Varies</td>
</tr>
<tr>
<td>R_A_TOV</td>
<td>Number</td>
<td>1000</td>
<td>E_D_TOV * 2 to 120000</td>
</tr>
<tr>
<td>E_D_TOV</td>
<td>Number</td>
<td>2000</td>
<td>1000 to R_A_TOV/2</td>
</tr>
<tr>
<td>WAN_TOV</td>
<td>Number</td>
<td>0</td>
<td>0 to R_A_TOV/4</td>
</tr>
<tr>
<td>MAX_HOPS</td>
<td>Number</td>
<td>7</td>
<td>7 to 19</td>
</tr>
</tbody>
</table>

4. Enter the portCfgLongDistance command, using the following syntax:

```
portcfglongdistance [slotnumber/]portnumber [distance_level]
[vc_translation_link_init] [desired_distance]
```

**slotnumber**
For blades, the slot number in which the blade is located. The slot number must be followed by a slash (/) and the port number. This option is not used for fixed-port switches.

**portnumber**
The port number.

**distance_level**
One of the following (the numerical value representing each distance_level is shown in parentheses):

- L0 (0): Specify L0 to configure the port to be a regular switch port.
- LE (3): Specify LE mode for distances up to 10 Km.
- LD (5): Specify LD for automatic long-distance configuration. The buffer credits for the given E_Port are automatically configured, based on the actual link distance measured during E_Port initialization.
- LS (6): Specify LS mode to configure a long-distance link with a buffer allocation based on a fixed desired distance value.

**vc_translation_link_init**
Enables the long-distance link initialization sequence. This extended link initialization sequence is an enhanced link reset protocol, and avoids excessive resetting of ports.

By default this option is set to 1 (enabled).

It must be set to 1 (enabled) when configuring a trunk over Extended Fabrics. It must be set to 1 for a long-distance link not configured for ISL R_RDY mode; otherwise, it must be reset to 0.

**desired_distance**
For an LD-mode link, desired_distance is a threshold limit for link distance to ensure buffer availability for other ports in the same port group. If the measured distance exceeds desired_distance, then desired_distance is used.

For an LS-mode link, desired_distance is used to calculate the buffers required for the port.

5. Repeat step 4 for the remote extended ISL port. Both the local and remote extended ISL ports must be configured to the same distance level. When the connection is initiated, the fabric will reconfigure.

The following example configures slot 1, port 1 for the LD link distance mode, enables the extended link initialization sequence, and sets the desired distance to 50 kilometers:

```
switch:admin> portcfglongdistance 1/1 LD 1 50
```
Table 82 lists the extended ISL modes for switches with Bloom-based ASICs. You can configure extended ISL modes with the `portCfgLongDistance` command when the Extended Fabrics license is activated.

### Table 82
Extended ISL modes: B-Series 2Gb Switches (Bloom and Bloom II ASICs)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Buffer allocation 1 Gbps</th>
<th>Distance @ 1 Gbps</th>
<th>Distance @ 2 Gbps</th>
<th>Earliest Fabric OS release</th>
<th>Extended Fabrics license required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>L0</td>
<td>5 (26)&lt;sup&gt;1&lt;/sup&gt;</td>
<td>10 km</td>
<td>5 km</td>
<td>All</td>
<td>No</td>
</tr>
<tr>
<td>LE</td>
<td>13</td>
<td>n/a</td>
<td>10 km</td>
<td>3.x, 4.x</td>
<td>No</td>
</tr>
<tr>
<td>LD&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Auto</td>
<td>Auto</td>
<td>Auto</td>
<td>Maximum is 200 km</td>
<td>3.1.0, 4.1.0, 4.4.0, 5.x (depending on the model)</td>
</tr>
<tr>
<td>LS&lt;sup&gt;3&lt;/sup&gt;</td>
<td>Based on user-specified distance</td>
<td>Based on user-specified distance</td>
<td>Based on user-specified distance</td>
<td>Maximum is 200 km</td>
<td>5.1.0</td>
</tr>
</tbody>
</table>

1. For each data channel (in this case, there are 4) there are 5 credits, plus 6 extra credits.
2. The dynamic long-distance mode (LD) automatically configures the number of buffer credits required, based on the actual link distance.
3. The static long-distance mode (LS) allocates the number of buffer credits based on the user-specified distance.
19 Administering ISL Trunking

This chapter contains procedures for using the ISL Trunking licensed feature, which optimizes the use of bandwidth by allowing a group of interswitch links to merge into a single logical link.

About ISL Trunking

ISL Trunking reduces or eliminates situations that require static traffic routes and individual ISL management to achieve optimal performance. Trunking optimizes fabric performance by distributing traffic across the shared bandwidth of all the interswitch links in a trunking group, allowing traffic to flow through any available link in a group rather than restricting it to a specific, potentially congested link. The use of trunking results in simplified fabric design and management, lowered cost of ownership, and increased data availability.

To use trunking, you must first install the ISL Trunking license. For details on obtaining and installing licensed features, see “Acquiring licensed features” on page 33. Trunking is enabled automatically when the ISL Trunking license is activated and ports are reinitialized (after installing the license, you enter the switchDisable and switchEnable commands), and trunks are easily managed using either Fabric OS CLI commands or Web Tools. You can enable and disable trunking and set trunk port speeds (for example, 2 Gbps, 4 Gbps, 8 Gbps, or autonegotiate) for entire switches or for individual ports.

Trunks distribute traffic dynamically and in order at the frame level, achieving greater performance with fewer interswitch links.

Trunks are compatible with both short wavelength (SWL) and long wavelength (LWL) fiber optic cables and transceivers.

Figure 30 illustrates how trunking can result in more throughput by distributing data over four ISLs with no congestion. In a fabric that does not have trunking capability, some paths would be congested and other paths under-utilized.

Figure 30 Distribution of traffic over ISL Trunking groups

Trunks operate best when the cable length of each trunked link is roughly equal to the others in the trunk. For optimal performance, no more than 30 meters difference is recommended.

Connections between the HP StorageWorks SAN Switch 4/32, 4/32B, 4/64 SAN Switch, Multi-protocol Router, the 4/256 SAN Director using the FC4-16/32/48, FC4-16IP, and the DC SAN Backbone Director (short name, DC Director) using the FC8-16/32/48 port blades support these advanced features:

- Up to eight ports in one trunk group to create high performance 32 Gbps ISL trunks between switches.
- ISL Trunking over longer distances than other models.
- Dynamic trunk master reassignment if a trunk master is disabled (on other platforms, all ports on a trunk must be disabled temporarily to reassign a master).
- 4 Gbps trunk links.
- 8 Gbps trunk links where supported.
The maximum number of ports per trunk and trunks per switch depends on the HP model.

**NOTE:** Director blade model FC10-6 does not support trunking.

For detailed information about trunking commands, see online help or the Fabric OS Command Reference.

### Standard trunking criteria

Observe the following criteria for standard distance trunking:

- There must be a direct connection between participating switches.
- Trunk ports must reside in the same port group.
- Trunk ports must run at the same speed (either 2 Gbps, 4 Gbps, or 8 Gbps).
- Trunk ports must be set to the same ISL mode (L0 is the default). For details on extended ISL mode.
- Trunk ports must be E_Ports or EX_Ports.
- For optimal performance, cable lengths of no more than 30 meters difference are recommended.
- The `switch.interopMode` parameter must be set to 0. See “Implementing an Interoperable Fabric” on page 505 for information and procedures related to interoperability mode.
- The port ISL mode must be disabled (using the `portCfgIslMode` command).

### EX_Port trunking

In Fabric OS 5.2.0 and later, you can configure EX_Ports to use frame-based trunking just like regular E_Ports. EX_Port frame based trunking has a “master” trunk link. If the master link goes down, the entire trunk will re-form and it will be taken offline for a short period of time. The EX_Port restrictions are the same as E_Ports. A trunk of E- or EX_Port can be up to 8-ports wide. All the ports must be adjacent to each other using the clearly marked groups on the front of the product.

### Fabric considerations

The ISL Trunking feature is provided with the Fabric OS and can be activated by entering a license key, available from HP. When the ISL Trunking license is activated (after you have entered the `switchDisable` and `switchEnable` commands), trunking is automatically implemented for any eligible ISLs.

A license must be activated on each switch that participates in trunking.

To use ISL Trunking in the fabric, the fabric must be designed to allow trunking groups to form. To identify the most useful trunking groups, evaluate the traffic patterns before designing or redesigning the fabric.

ISL Trunking can be used to simplify storage area network design and improve performance. When designing the SAN, consider the following recommendations in addition to the standard guidelines for SAN design:

- Evaluate the traffic patterns within the fabric.
- Place trunking-capable switches adjacent to each other.
  This maximizes the number of trunking groups that can form. If you are using a core/edge topology, place trunking-capable switches at the core of the fabric and any switches that are not trunking-capable at the edge of the fabric.
- Activate an ISL Trunking license on each switch that is to participate in a trunking group.
- When connecting two switches with two or more ISLs, ensure that all trunking requirements are met to allow a trunking group to form.
• Determine the optimal number of trunking groups between each set of linked switches, depending on traffic patterns and port availability.

The goal is to avoid traffic congestion without unnecessarily using ports that could be used to attach other switches or devices. Consider these points:

• Each physical ISL uses two ports that could otherwise be used to attach node devices or other switches.
• Trunking groups can be used to resolve ISL oversubscription if the total capability of the trunking group is not exceeded.
• Consider how the addition of a new path will affect existing traffic patterns:
  • A trunking group has the same link cost as the master ISL of the group, regardless of the number of ISLs in the group. This allows slave ISLs to be added or removed without causing data to be rerouted, because the link cost remains constant.
  • The addition of a path that is shorter than existing paths causes traffic to be rerouted through that path.
  • The addition of a path that is longer than existing paths may not be useful because the traffic will choose the shorter paths first.
• Plan for future bandwidth addition to accommodate increased traffic.

For trunking groups over which traffic is likely to increase as business requirements grow, consider leaving one or two ports in the group available for future nondisruptive addition of bandwidth.
• Consider creating redundant trunking groups where additional ports are available or paths are particularly critical.

This helps to protect against oversubscription of trunking groups, multiple ISL failures in the same group, and the rare occurrence of an ASIC failure.
• To provide the highest level of reliability, deploy trunking groups in redundant fabrics to further ensure ISL failures do not disrupt business operations.

### Initializing trunking on ports

After you unlock the ISL Trunking license, you must reinitialize the ports being used for ISLs so that they recognize that trunking is enabled. This procedure only needs to be performed one time.

To reinitialize the ports, you can either disable and then re-enable the switch, or disable and then re-enable the affected ports.

To disable and re-enable the switch:

1. Connect to the switch and log in as admin.
2. Enter the `switchDisable` command.
3. Enter the `switchEnable` command.

To disable and re-enable ports:

1. Connect to the switch and log in as admin.
2. Enter the `portDisable` command. The format is:
   ```
   portDisable [slot/]port
   ```
   On directors, `slot` is the slot number and `port` is the port number of the port you want to disable.
3. Enter the `portEnable` command. The format is:
   ```
   portEnable [slot/]port
   ```
   On directors, `slot` is the slot number and `port` is the port number of the port you want to enable.

### Monitoring traffic

To implement ISL Trunking effectively, you must monitor fabric traffic to identify congested paths or to identify frequently dropped links. While monitoring changes in traffic patterns, you can adjust the fabric design accordingly, such as by adding, removing, or reconfiguring ISLs and trunking groups in problem areas.
There are three methods of monitoring fabric traffic:

- Advanced Performance Monitoring monitors traffic flow and allows you to view the impact of different fabric configurations on performance. See “Administering Advanced Performance Monitoring” on page 361 for additional information.

- Fabric Watch allows you to monitor traffic flow through specified ports on the switch and send alerts when the traffic exceeds or drops below configured thresholds. See the Fabric Watch Administrator’s Guide for additional information.

- Use the portPerfShow command as described in the following procedure to record traffic volume for each port in your fabric over time.

To use the portPerfShow command:

1. Connect to the switch and log in as admin.
2. Enter the following command:
   ```sh
guest:admin> portperfshow [interval]
   ```
   where interval is the number of seconds between each data-gathering sample (the default is one sample every second).

3. Record the traffic flow for each port participating in an ISL.
4. Repeat step 1 through step 3 for each switch in the fabric until all ISL traffic flow is captured.

   In a large fabric, it may be necessary to only identify and capture the key ISLs. However, you may want to continue this process throughout the day (or an entire work cycle), to capture varying traffic patterns under different conditions.

The following example shows a switch without trunking, and indicates that ports 0 through 2 are under utilized and ports 4 and 5 are congested:

```
switch:admin> portperfshow
  0 1 2 3 4 5 6 7 Total
  --------------------------------- 
  0 0 0 145m 204m 202m 0 168m 719
  0 0 0 145m 206m 208m 0 186m 745
```

The following example shows traffic flowing through a trunking group (ports 5, 6, and 7). After port 6 fails, traffic is redistributed over the remaining two links in the group, ports 5 and 7:

```
switch:admin> portperfshow
  0 1 2 3 4 5 6 7 Total
  --------------------------------- 
  0 0 0 0 0 145m 144m 145m 434
  0 0 0 0 0 144m 143m 144m 431
  0 0 0 0 0 162m 0 162m 324
  0 0 0 0 0 186m 0 186m 372
  0 0 0 0 0 193m 0 192m 385
  0 0 0 0 0 202m 0 202m 404
  0 0 0 0 0 209m 0 209m 418
```
Enabling and disabling ISL Trunking

You can enable or disable ISL Trunking for a single port or for an entire switch. When you execute the commands `portCfgTrunkPort` or `switchCfgTrunk` to update the trunking configuration, the ports for which the configuration applies are disabled and re-enabled with the new trunk configuration. As a result, traffic through those ports could be disrupted.

**IMPORTANT:** Trunking is performed based on QoS configuration on the master and the slave ports. That is, in a given trunk group, if there are some ports with QoS enabled and some with QoS disabled, they would form two different trunks, one with QoS enabled and the other with QoS disabled.

To enable or disable ISL Trunking on one port:

1. Connect to the switch and log in as admin.
2. Enter the `portCfgTrunkPort` command. The format is:
   ```
   portcfgtrunkport [slotnumber/]portnumber mode
   ```
   - `slotnumber`: Specifies the number of the slot in which the port blade containing the port is located. This operand only required for Brocade directors.
   - `portnumber`: Specifies the number of the port on which you want to enable or disable trunking.
   - `mode`: Enables (1) or disables (0) trunking on the specified port.

   The following example enables trunking on slot 1, port 3:
   ```
   switch:admin> portcfgtrunkport 1/3 1
done.
   switch:admin>
   ```

To enable or disable ISL Trunking for all of the ports on a switch:

1. Connect to the switch and log in as admin.
2. Enter the `switchCfgTrunk` command. The format is:
   ```
   switchcfgtrunk mode
   ```
   - Mode 1 enables and mode 0 disables ISL Trunking for all ports on the switch.

   The following example enables trunking all ports in the switch.
   ```
   switch:admin> switchcfgtrunk 1
   Committing configuration...done.
   switch:admin>
   ```
Setting port speeds

For long-distance ports, if a port is set to autonegotiate port speed, the maximum speed (which is 4 Gbps) is assumed for reserving buffers for the port—this wastes buffers if the port is actually running at 2 Gbps. For long-distance ports, it is best to set the port speed (this applies to the 4/32 SAN Switch, 4/32B SAN Switch and the 4/256 SAN Director only).

**IMPORTANT:** 8 Gbps is only supported between 4/256 SAN Directors-to-DC Directors or between DC Director-to-DC Directors with the appropriate blades and 8 Gbps supported SFPs installed.

You can set the port speed for one port or for an entire switch. Trunked ports must be set to the same speed.

To set the speed for one port:
1. Connect to the switch and log in as admin.
2. Enter the `portCfgSpeed` command. The format is:
   
   ```
   portcfgspeed [slotnumber/]portnumber, speed_level
   ```

   - **slotnumber** For bladed systems only, specify the slot number of the port to be configured, followed by a slash (/). This operand is only required for Brocade directors.
   - **portnumber** Specifies the port number relative to its slot for bladed systems.
   - **speedlevel** Specifies the speed of the link:
     - 0—Autonegotiating mode. The port automatically configures for the highest speed.
     - 1—one Gbps mode. Fixes the port at a speed of one Gbps. Changing the speed to one Gbps causes the port to be excluded from the trunk group.
     - 2—two Gbps mode. Fixes the port at a speed of two Gbps.
     - 8—eight Gbps mode. Fixes the port at a speed of four Gbps. (4/256 SAN Director and DC Directors with supported blades and 8 Gbps SFPs installed only.)

   The following example sets the speed for port 3 on slot 2 to two Gbps:
   
   ```
   switch:admin> portcfgspeed 2/3 2
   done.
   switch:admin>
   ```

   The following example sets the speed for port 3 on slot 2 to autonegotiate:
   
   ```
   switch:admin> portcfgspeed 2/3 0
   done.
   switch:admin>
   ```

To set the same speed for all ports on the switch:
1. Connect to the switch and log in as admin.
2. Enter the `switchCfgSpeed` command. The format is:
   
   ```
   switchCfgSpeed speedlevel
   ```
The following example sets the speed for all ports on the switch to two Gbps:

```
switch:admin> switchcfgspeed 2
Committing configuration...done.
```

The following example sets the speed for all ports on the switch to autonegotiate:

```
switch:admin> switchcfgspeed 0
Committing configuration...done.
```

### Displaying trunking information

The `trunkShow` command offers an efficient means of listing out all the trunks and members of a trunk. You can easily discover the peer ports for disabling a port, disconnecting or adding additional members. Viewing trunks is also useful for when you want to ensure that trunks are formed correctly.

Use the `trunkShow` command to display the following information about ISL Trunking groups:

- Number identifier.
- Port-to-port connections, listed in the following format: `local port number -> remote port number`.
- WWNs of the remote switches.
- Deskew values (the time difference, in nanoseconds divided by 10, for traffic to travel over each ISL as compared to the shortest ISL in the group). The system automatically sets the minimum deskew value of the shortest ISL to 15.
- Master ports.

To display trunking information:

1. Connect to the switch and log in as admin.
2. Enter the `trunkShow` command.

This example shows three trunking groups (1, 2, and 3); ports 1, 4, and 14 are masters:

```
switch:admin> trunkshow
1: 1 -> 1 10:00:00:60:69:04:10:83 deskew 16 Master
   0 -> 0 10:00:00:60:69:04:10:83 deskew 15
2: 4 -> 4 10:00:00:60:69:04:01:94 deskew 16 Master
   5 -> 5 10:00:00:60:69:04:01:94 deskew 15
   7 -> 7 10:00:00:60:69:04:01:94 deskew 17
   6 -> 6 10:00:00:60:69:04:01:94 deskew 16
3:14 -> 14 10:00:00:60:69:04:10:83 deskew 16 Master
   15 -> 15 10:00:00:60:69:04:10:83 deskew 15
```
Trunking over Extended Fabrics

In addition to the criteria listed in “Standard trunking criteria” on page 378, observe the following criteria for trunking over Extended Fabrics:

- ISL Trunking over Extended Fabrics is supported on switches running Fabric OS 4.4.0 and later.
- Extended Fabrics and ISL Trunking licenses are required on all participating switches.
- The `vc_translation_link_init` parameter must be set the same on all ports in an extended trunk.
**Trunking distances**

Enhanced trunking support for switches with Condor ASICs is summarized in Table 82.

**Table 82**  Trunking support for SAN Switch 4/32, 4/32B and 4/64 SAN Switch (Condor ASIC)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Distance</th>
<th>Number of 2 Gbps ports</th>
<th>Number of 4 Gbps ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>LE</td>
<td>10 km</td>
<td>32 (four 8-port trunks)</td>
<td>32 (four 8-port trunks)</td>
</tr>
<tr>
<td>L0.5</td>
<td>25 km</td>
<td>32 (four 8-port trunks)</td>
<td>15 (one 8-port trunk)</td>
</tr>
<tr>
<td>L1</td>
<td>50 km</td>
<td>15 (one 2-port trunk)</td>
<td>7 (one 7-port trunk)</td>
</tr>
<tr>
<td>L2</td>
<td>100 km</td>
<td>7 (one 7-port trunk)</td>
<td>3 (one 3-port trunk)</td>
</tr>
<tr>
<td>LD</td>
<td>200 km</td>
<td>3 (one 3-port trunk)</td>
<td>0</td>
</tr>
<tr>
<td>LD</td>
<td>250 km</td>
<td>3 (one 3-port trunk)</td>
<td>0</td>
</tr>
<tr>
<td>LD</td>
<td>500 km</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Enhanced trunking support for the FC4-48 port blade in the 4/256 SAN Director is summarized in Table 83.

**Table 83**  Trunking support for 4/256 SAN Director and DC Directors with supported blades (Condor and Condor2 ASIC)

<table>
<thead>
<tr>
<th>Mode</th>
<th>Distance</th>
<th>Number of 2 Gbps ports</th>
<th>Number of 4 or 8 Gbps ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>LE</td>
<td>10 km</td>
<td>48 (six 8-port trunks)</td>
<td>48 (six 8-port trunks)</td>
</tr>
<tr>
<td>L0.5</td>
<td>25 km</td>
<td>48 (six 8-port trunks)</td>
<td>22 (one 8-port trunk and one 3-port trunk per Condor)</td>
</tr>
<tr>
<td>L1</td>
<td>50 km</td>
<td>22 (one 8-port trunk and one 3-port trunk per Condor)</td>
<td>10 (one 5-port trunk per Condor)</td>
</tr>
<tr>
<td>L2</td>
<td>100 km</td>
<td>10 (one 5-port trunk per Condor)</td>
<td>4 (one 2-port trunk per Condor)</td>
</tr>
<tr>
<td>LD</td>
<td>200 km</td>
<td>4 (one 2-port trunk per Condor)</td>
<td>0</td>
</tr>
<tr>
<td>LD</td>
<td>250 km</td>
<td>4 (one 2-port trunk per Condor)</td>
<td>0</td>
</tr>
<tr>
<td>LD</td>
<td>500 km</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Troubleshooting trunking problems**

If you have difficulty with trunking, try the solutions in this section.

**Listing link characteristics**

If a link that is part of an ISL Trunk fails, use the `trunkDebug` command to troubleshoot the problem, as shown in the following procedure.

1. Connect to the switch and log in as admin.
2. Enter the following command:
   ```
   trunkDebug port, port
   port     Specifies the number of a port in an ISL Trunking group.
   ```

The `trunkDebug` command displays the possible reason that two ports cannot be trunked. Possible reasons are:

- The switch does not support trunking.
- A trunking license is required.
- Trunking is not supported in switch interoperability mode.
• Port trunking is disabled.
• The port is not an E_Port.
• The port is not 2 Gbps, 4 Gbps, or 8 Gbps.
• The port connects to different switches.
• The ports are not the same speed, or they are not set to a valid speed.
• The ports are not set to the same long distance mode.
• Local or remote ports are not in the same port group.
• The difference in the cable length among trunked links is greater than the allowed difference.

This example shows that port 3 is not configured as an E_Port:

```
switch:admin> trunkdebug 3 5
port 3 is not E port
```

Recognizing buffer underallocation

A port disabled at one end because of buffer underallocation causes all the disabled ports at the other end to become enabled. Some of these enabled ports become disabled due to a lack of buffers, which in turn triggers ports to be enabled once again at the other end. While the system is stabilizing the buffer allocation, it warns that ports are disabled due to lack of buffers, but it does not send a message to the console when buffers are enabled. The system requires a few passes to stabilize the buffer allocation. Ultimately, the number of ports for which buffers are available come up and stabilize. You should wait for stabilization, and then proceed with correcting the buffer allocation situation.

To get out of buffer-limited mode on E_Ports or LD_Ports:

1. Change the LD/L1/L2/L0.5 port speed to a lower speed (of non-buffer limited ports).
2. Change the LD port’s estimated distance to a shorter distance (of non-buffer limited ports).
3. Change LD/L1/L2/L0.5 back to L0 (of non-buffer limited ports).
4. If you are in buffer-limited mode on the LD port, then increase the estimated distance.
5. Enable any of these changes on the buffer-limited port or switch by issuing the commands `portDisable` and `portEnable`.

Reconfiguring a port to LD from another mode can result in the port being disabled for lack of buffers—this does not apply to the SAN Switch 4/32, 4/32B and 4/256 SAN Director (using FC4-16 and FC4-32 port blades).

If this happens:

• In Fabric OS 4.2.x, reconfigure the disabled LD port back to the original mode.
• In Fabric OS 4.4.0 and later, specify a slightly shorter distance for the `desired_distance` parameter in the `portCfgLongDistance` command.
About zoning

Zoning enables you to partition your SAN into logical groups of devices that can access each other. A device can communicate only with other devices connected to the fabric within its specified zone. For example, you can partition your SAN into two zones, winzone and unixzone, so that your Windows servers and storage do not interact with your UNIX servers and storage. When zoning is enabled, devices that are not included in a zone configuration are inaccessible to other devices in the fabric.

Zones can be configured dynamically. They can vary in size, depending on the number of fabric-connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

When using a mixed fabric—that is, a fabric containing two or more switches running different fabric operating systems—you should use the switch with the highest Fabric OS level to perform zoning tasks.

You must install Advanced Zoning licenses on all the switches in the fabric before attempting to configure zones. If a Zoning license is removed, you must make sure it is reinstalled properly on the affected switch before attempting the \texttt{cfgEnable} zoning operation. Failure to follow these steps can cause inconsistency of the zoning configuration on the affected switches should a zoning operation be attempted from a remote switch in the fabric. On the affected switches, an error message indicates that the Zoning license is missing.

You can use zones to logically consolidate equipment for efficiency or to facilitate time-sensitive functions; for example, use zoning to create a temporary zone to back up nonmember devices.

Any zone object connected to the fabric can be included in one or more zones. Zone objects can communicate only with objects within the same zone. For example, consider Figure 31, which shows configured zones, Red, Green, and Blue.

- Server 1 can communicate only with the Loop 1 devices.
- Server 2 can communicate only with the RAID and Blue zone devices.
- Server 3 can communicate with the RAID device and the Loop 1 device.
- The Loop 2 JBODs are not assigned to a zone; no other zoned fabric device can access them.

![Figure 31 Zoning example](image)

To list the commands associated with zoning, use the \texttt{zoneHelp} command. For detailed information on the zoning commands used in the procedures, see the \textit{Fabric OS Command Reference} or the online man page for each command.

Before using the procedures, you should become familiar with the zoning concepts described in the following sections.
Zone types

Table 84 summarizes the types of zoning available.

Table 84  Types of zoning

<table>
<thead>
<tr>
<th>Zone type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage-based</td>
<td>Storage units typically implement LUN-based zoning, also called LUN masking. LUN-based zoning limits access to the LUNs on the storage port to the specific WWN of the server HBA. It is needed in most SANs. It functions during the probe portion of SCSI initialization. The server probes the storage port for a list of available LUNs and their properties. The storage system compares the WWN of the requesting HBA to the defined zone list, and returns the LUNs assigned to the WWN. Other LUNs on the storage port are not made available to the server.</td>
</tr>
<tr>
<td>Host-based</td>
<td>Host-based zoning can implement WWN or LUN masking.</td>
</tr>
<tr>
<td>Fabric-based</td>
<td>Fabric switches implement fabric-based zoning, in which the zone members are identified by WWN or port location in the fabric. Fabric-based zoning is also called name server-based or soft zoning. When a device queries the fabric name server, the name server determines the zones in which the device belongs. The server returns information on all members of the zones in the fabric to the device. Devices in the zone are identified by node WWN, port WWN, or domain,port of the switch to which the device is connected. The primary approaches to fabric-based zoning are summarized in Table 85.</td>
</tr>
</tbody>
</table>

NOTE: Fabric OS has several types of zones that do not behave like the “regular” zones described here. These special zones include broadcast zones, Traffic Isolation zones, and QoS zones. See “Broadcast zones” on page 395, “Traffic isolation” on page 333, and “QoS: SID/DID traffic prioritization” on page 340 for information about these special zones.

Table 85 lists the various approaches you can take when implementing zoning in a fabric.

Table 85  Approaches to fabric-based zoning

<table>
<thead>
<tr>
<th>Zoning approach</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single HBA</td>
<td>Zoning by single HBA most closely re-creates the original SCSI bus. Each zone created has only one HBA (initiator) in the zone; each of the target devices is added to the zone. Typically, a zone is created for the HBA and the disk storage ports are added. If the HBA also accesses tape devices, a second zone is created with the HBA and associated tape devices in it. In the case of clustered systems, it could be appropriate to have an HBA from each of the cluster members included in the zone; this is equivalent to having a shared SCSI bus between the cluster members and assumes that the clustering software can manage access to the shared devices. In a large fabric, zoning by single HBA requires the creation of possibly hundreds of zones; however, each zone contains only a few members. Zone changes affect the smallest possible number of devices, minimizing the impact of an incorrect zone change. This zoning philosophy is the preferred method.</td>
</tr>
</tbody>
</table>

Recommended approach

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
</table>
A zone object is any device in a zone, such as:

- Physical port number or port index on the switch
- Node World Wide Name (N-WWN)
- Port World Wide Name (P-WWN)

Zone objects identified by port number or index number are specified as a pair of decimal numbers in the form $d, index$ (where $d$ is the Domain ID of the switch and $index$ is the index number on that switch in relation to the port you want to specify).

For example, in Directors, “4,30” specifies port 14 in slot number 2 (Domain ID 4, port index 30). On fixed-port models, “3,13” specifies port 13 in switch Domain ID 3.

When a zone object is the physical port number, then all devices connected to that port are in the zone.

World Wide Names are specified as 8-byte (16-digit) hexadecimal numbers, separated by colons (:) for example, 10:00:00:90:69:00:00:8a.

When a zone object is the node WWN name, only the specified device is in the zone.

### Table 85 Approaches to fabric-based zoning (continued)

<table>
<thead>
<tr>
<th>Zoning approach</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alternative approaches</strong></td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Zoning by application typically requires zoning multiple, perhaps incompatible, operating systems into the same zones. This method of zoning creates the possibility that a minor server in the application suite could disrupt a major server (such as a Web server disrupting a data warehouse server). Zoning by application can also result in a zone with a large number of members, meaning that more notifications, such as registered state change notifications (RSCNs), or errors, go out to a larger group than necessary.</td>
</tr>
<tr>
<td>Operating system</td>
<td>Zoning by operating system has issues similar to zoning by application. In a large site, this type of zone can become very large and complex. When zone changes are made, they typically involve applications rather than a particular server type. If members of different operating system clusters can see storage assigned to another cluster, they might attempt to own the other cluster’s storage and compromise the stability of the clusters.</td>
</tr>
<tr>
<td>Port allocation</td>
<td>Avoid zoning by port allocation unless the administration team has very rigidly enforced processes for port and device allocation in the fabric. It does, however, provide some positive features. For instance, when a storage port, server HBA, or tape drive is replaced, the change of WWN for the new device is of no consequence. As long as the new device is connected to the original port, it continues to have the same access rights. The ports on the edge switches can be pre-associated to storage ports, and control of the fan-in ratio (the ratio of the input port to output port) can be established. With this pre-assigning technique, the administrative team cannot overload any one storage port by associating too many servers with it.</td>
</tr>
<tr>
<td><strong>Not recommended</strong></td>
<td></td>
</tr>
<tr>
<td>No fabric zoning</td>
<td>Using no fabric zoning is the least desirable zoning option because it allows devices to have unrestricted access on the fabric. Additionally, any device attached to the fabric, intentionally or maliciously, likewise has unrestricted access to the fabric. This form of zoning should be utilized only in a small and tightly controlled environment, such as when host-based zoning or LUN masking is deployed.</td>
</tr>
</tbody>
</table>
When a zone object is the port WWN name, only the single port is in the zone.

The types of zone objects used to define a zone can be mixed. For example, a zone defined with the zone objects 2,12; 2,14; 10:00:00:80:33:3f:aa:11 contains the devices connected to domain 2, ports 12 and 14, and a device with the WWN (either node name or port name) 10:00:00:80:33:3f:aa:11 that is connected on the fabric.

Zoning schemes

You can establish a zone by identifying zone objects using one or more of the following zoning schemes:

- **Domain,index**—All members are specified by Domain ID, port number, or domain, index number pair or aliases, described in “Zone aliases” on page 390.
- **World Wide Name (WWN)**—All members are specified only by World Wide Name (WWNs) or aliases of WWNs. They can be node or port versions of the WWN.
- **Mixed zoning**—A zone containing members specified by a combination of domain,port or domain,index, and WWN.

**NOTE:** If your fabric has a switch with a Fabric OS version earlier than 5.2.0, you cannot use domain,port zoning with port numbers of 256 or greater. You must use WWN zoning instead.

Zone aliases

A zone alias is a name assigned to a device or a group of devices. By creating an alias, you can assign a familiar name to a device or group multiple devices into a single name. This simplifies cumbersome data entry and allows an intuitive naming structure (such as using “NT_Hosts” to define all NT hosts in the fabric).

Zone aliases also simplify repetitive entry of zone objects such as port numbers or a WWN. For example, you can use the name “Eng” as an alias for “10:00:00:80:33:3f:aa:11”.

Naming zones for the initiator they contain can also be useful. For example, if you use the alias SRV_MAILSERVER_SLT5 to designate a mail server in PCI slot 5, then the alias for the associated zone is ZNE_MAILSERVER_SLT5. This clearly identifies the server host bus adapter (HBA) associated with the zone.

Zone configuration naming is flexible. One configuration should be named PROD_fabricname, where fabricname is the name that the fabric has been assigned. The purpose of the PROD configuration is to easily identify the configuration that can be implemented and provide the most generic services. If other configurations are used for specialized purposes, names such as “BACKUP_A,” “RECOVERY_2,” and “TEST_18jun02” can be used.

Zone configurations

A zone configuration is a group of one or more zones. A zone can be included in more than one zone configuration. When a zone configuration is in effect, all zones that are members of that configuration are in effect.

Several zone configurations can reside on a switch at once, and you can quickly alternate between them. For example, you might want to have one configuration enabled during the business hours and another enabled overnight. However, only one zone configuration can be enabled at a time.

The different types of zone configurations are:

- **Defined Configuration**—The complete set of all zone objects defined in the fabric.
- **Effective Configuration**—A single zone configuration that is currently in effect. The effective configuration is built when you enable a specified zone configuration.
- **Saved Configuration**—A copy of the defined configuration plus the name of the effective configuration, which is saved in flash memory by the cfgSave command. (You can also use the configUpload command to provide a backup of the zoning configuration and the configDownload command to restore the zoning configuration.) There might be differences between the saved configuration and the defined configuration if you have modified any of the zone definitions and have not saved the configuration.
• **Disabled Configuration**—The effective configuration is removed from flash memory.

When you disable the effective configuration, the Advanced Zoning feature is disabled on the fabric, and all devices within the fabric can communicate with all other devices (unless you previously set up a default zone, as described in “Activating default zones” on page 403). This does not mean that the zoning database is deleted, however, only that there is no configuration active in the fabric.

On power-up, the switch automatically reloads the saved configuration. If a configuration was active when it was saved, the same configuration is reinstated on the local switch with an autorun of the `cfgEnable` command.

### Zoning enforcement

Zoning enforcement describes a set of predefined rules that the switch uses to determine where to send incoming data. There are two methods of enforcement: software-enforced and hardware-enforced zoning.

Zoning enables you to restrict access to devices in a fabric. Software-enforced zoning prevents hosts from discovering unauthorized target devices, while hardware-enforced zoning prevents a host from accessing a device it is not authorized to access.

#### Software-enforced zoning

Software-enforced zoning is used for any mixed zone (a zone with both WWN and `domain,port` members).

Software-enforced zoning:

- Is also called “soft zoning,” “name server zoning,” “fabric-based zoning,” or “session-based zoning.”
- Is available on 1, 2, 4, 8 and 10 Gbps platforms.
- Prevents hosts from discovering unauthorized target devices.
- Ensures that the name server does not return any information to an unauthorized initiator in response to a name server query.
- Does not prohibit access to the device. If an initiator has knowledge of the network address of a target device, it does not need to query the name server to access it, which could lead to undesired access to a target device by unauthorized hosts.
- Is exclusively enforced through selective information presented to end nodes through the fabric Simple Name Server (SNS). When an initiator queries the name server for accessible devices in the fabric, the name server returns only those devices that are in the same zone as the initiator. Devices that are not part of the zone are not returned as accessible devices.

#### Hardware-enforced zoning

Hardware-enforced zoning means that each frame is checked by hardware (the ASIC) before it is delivered to a zone member and is discarded if there is a zone mismatch. When hardware-enforced zoning is active, the HP switch monitors the communications and blocks any frames that do not comply with the effective zone configuration. The switch performs this blocking at the transmit side of the port on which the destination device is located.

Hardware-enforced zoning is in effect when all of the members of a zone are identified the same way, either using WWNs or `domain,port` notation.

If a zone does not have either all WWN or all `domain,port` entries, then software-enforced zoning is in effect.

For overlapping zones (in which zone members appear in two or more zones), hardware-enforced zoning is in effect as long as the overlapping zones have either all WWN or all `domain,port` entries.

Hardware-enforced zoning:

- Is also called hard zoning or ASIC-enforced zoning.
- Prevents a host from discovering unauthorized target devices.
- Prevents a host from accessing a device it is not authorized to access.
- Is enforced at the ASIC level. Each ASIC maintains a list of source port IDs that have permission to access any of the ports on that ASIC.
• Is available on 1, 2, 4, 8 and 10 Gbps platforms.
• Ensures that the name server does not return any information to an unauthorized initiator in response to a name server query.
• Is exclusively enforced through selective information presented to end nodes through the fabric Simple Name Server (SNS). When an initiator queries the name server for accessible devices in the fabric, the name server returns only those devices that are in the same zone as the initiator. Devices that are not part of the zone are not returned as accessible devices.

Fabric OS uses hardware-enforced zoning (on a per-zone basis) whenever the fabric membership or zone configuration changes.

The exact zoning methodology varies on different switch models. Table 86 shows various HP switch models, the hardware zoning methodology for each, and tips for best usage.

Table 86  Enforcing hardware zoning

<table>
<thead>
<tr>
<th>Fabric type</th>
<th>Methodology</th>
<th>Best practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade 2000-series</td>
<td>Enable hardware-enforced zoning only on domain,port zones; WWN or mixed zones are not hardware-enforced. Any domain,port zone that overlaps a mixed or WWN zone is not hardware-enforced. An overlap occurs when a member specified by WWN is connected to a port in a domain,port zone. The domain,port zone loses its hardware enforcement even though a review of the zone configuration does not indicate it.</td>
<td>Use domain,port identifiers. Do not identify a zone member by its WWN.</td>
</tr>
<tr>
<td>HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP c-Class BladeSystem, SAN Switch 4/32, 4/64 SAN Switch, SAN Switch 4/32B, 400 MP Router, 4/256 SAN Director, and the DC SAN Backbone Director (short name, DC Director)</td>
<td>Enable hardware-enforced zoning on domain,port zones, and WWN zones. Overlap of similar zone types does not result in the loss of hardware enforcement. Overlap with other zone type results in the loss of hardware enforcement. As in the Brocade 2000-series switches, connecting a device specified by WWN to a port specified in a domain,port zone results in loss of the hardware enforcement in both zones. <strong>For the 4/256 SAN Director with an FC4-48 port blade and the DC Director with an FC8-48 port blade:</strong> If ports 16 through 47 on the FC4-48 port blade use domain,port identifiers, then session-based zoning is enforced on these ports.</td>
<td>Use either WWN or domain,port identifiers.</td>
</tr>
<tr>
<td>Mixed switches</td>
<td>Enable hardware-enforced zoning according to each switch type. Use the portZoneShow command to find the zone type to which a device is attached.</td>
<td>Use domain,port identifiers. You can use WWN identifiers if you place disk and tape targets on HP 2Gb and SAN Director 2/128 models, and do not use domain,port identifiers.</td>
</tr>
</tbody>
</table>
Figure 32 shows a fabric with four hardware-enforced zones that don’t overlap.

Figure 32 Hardware-enforced nonoverlapping zones

Figure 33 shows the same fabric components, but with overlapping zones.

Figure 33 Hardware-enforced overlapping zones

Any zone using a mixed zoning scheme on the 2 Gbps platform relies on name server authentication as well as hardware-assisted (ASIC) authentication, which ensures that any PLOGI/ADISC/PDISC/ACC from an unauthorized device attempting to access a device it is not zoned with is rejected. HP 2Gb switches always deploy the hardware assist, in any zone configuration (see Figure 34 and Figure 35).

Figure 34 Zoning with hardware assist (mixed-port and WWN zones)
In Figure 35, only the overlapping ports are software-enforced with hardware assist.

Considerations for zoning architecture

Table 87 lists considerations for zoning architecture.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of zoning:</td>
<td>If security is a priority, hard zoning is recommended.</td>
</tr>
<tr>
<td>hard or soft (session-based)</td>
<td></td>
</tr>
<tr>
<td>Use of aliases</td>
<td>The use of aliases is optional with zoning. Using aliases requires structure when defining zones. Aliases will aid administrators of zoned fabric in understanding the structure and context.</td>
</tr>
<tr>
<td>Interoperability Fabric</td>
<td>If the fabric includes a third-party switch product, only WWN zoning is supported. Other types of zoning, including QuickLoop, are not supported.</td>
</tr>
<tr>
<td>QLFA zones</td>
<td>Evaluate if the fabric will have QuickLoop Fabric Assist (QLFA) or QuickLoop (QL) in it, and consider the following items before creating and setting up QLFA zones:</td>
</tr>
<tr>
<td></td>
<td>QuickLoop Zoning—QuickLoop/QuickLoop zones cannot run on Fabric OS 4.1.0 or later. However, Fabric OS can manage (create, remove, update) QL zones.</td>
</tr>
<tr>
<td></td>
<td>QuickLoop Fabric Assist—A switch running Fabric OS 4.1.0 or later cannot have a Fabric Assist host directly connected to it. However, such a switch can be part of a Fabric Assist zone if a Fabric Assist host is connected to a compatible switch in the fabric.</td>
</tr>
<tr>
<td>Testing</td>
<td>Before implementing a new zone, you should run the Zone Analyzer from Web Tools to isolate any possible problems. This is especially useful as fabrics increase in size.</td>
</tr>
</tbody>
</table>
The zone configuration is managed on a fabric basis. Zoning can be implemented and administered from any switch in the fabric (it is best to use a newer switch such as the SAN Switch 4/32B, 4/64 SAN Switch, or a Director) that has an Advanced Zoning license enabled. When a change in the configuration is saved, enabled, or disabled according to the transactional model, it is automatically (by closing the transaction) distributed to all switches in the fabric, preventing a single point of failure for zone information.

**NOTE:** Zoning commands make changes that affect the entire fabric. When executing fabric-level configuration tasks, allow time for the changes to propagate across the fabric before executing any subsequent commands. For a large fabric, you should wait several minutes between commands.

### Best practices for zoning

The following are recommendations for using zoning:

- Always zone using the highest Fabric OS-level switch.
  Switches with lower Fabric OS versions do not have the capability to view all the functionality that a newer Fabric OS provides, as functionality is backwards compatible but not forwards compatible.
- Zone using the core switch versus an edge switch.
- Zone using a Director over a switch.
  A Director has more resources to handle zoning changes and implementations.

### Broadcast zones

Fibre Channel allows sending broadcast frames to all Nx_Ports if the frame is sent to a broadcast well-known address (FFFFFF); however, many target devices and HBAs cannot handle broadcast frames. To control which devices receive broadcast frames, you can create a special zone, called a broadcast zone, which restricts broadcast packets to only those devices that are members of the broadcast zone.

If there are no broadcast zones or if a broadcast zone is defined but not enabled, broadcast frames are not forwarded to any F_Ports. If a broadcast zone is enabled, broadcast frames are delivered only to those logged-in Nx_Ports that are members of the broadcast zone and are also in the same zone (regular zone) as the sender of the broadcast packet.

Devices that are not members of the broadcast zone can send broadcast packets, even though they cannot receive them.

A broadcast zone can have domain, port, WWN, and alias members.

Broadcast zones do not function in the same way as other zones. A broadcast zone does not allow access within its members in any way. If you want to allow or restrict access between any devices, you must create regular zones for that purpose. If two devices are not part of a regular zone, they cannot exchange broadcast or unicast packets.
To restrict broadcast frames reaching broadcast-incapable devices, create a broadcast zone and populate it with the devices that are capable of handling broadcast packets. Devices that cannot handle broadcast frames must be kept out of the broadcast zone so that they do not receive any broadcast frames.

You create a broadcast zone the same way you create any other zone except that a broadcast zone must have the name “broadcast” (case-sensitive). You can set up and manage broadcast zones using the standard zoning commands, which are described in “Creating and maintaining zones” on page 400.

**Supported switches for broadcast zones**

Broadcast zoning is enforced only for Fabric OS 5.3.x or later switches. If the fabric contains switches running Fabric OS versions earlier than 5.3.x, then all devices connected to those switches receive broadcast packets, even if they are not members of a broadcast zone.

**Broadcast zones and Admin Domains**

Each Admin Domain can have only one broadcast zone. However, all of the broadcast zones from all of the Admin Domains are considered as a single consolidated broadcast zone.

Broadcast packets are forwarded to all the ports that are part of the broadcast zone for any Admin Domain, have membership in that Admin Domain, and are zoned together (in a regular zone) with the sender of the broadcast frame.

**Figure 36** illustrates how broadcast zones work with Admin Domains. **Figure 36** shows a fabric with five devices and two Admin Domains, AD1 and AD2. Each Admin Domain has two devices and a broadcast zone.

![Diagram showing broadcast zones and Admin Domains](image)

**Figure 36** Broadcast zones and Admin Domains

The dotted box represents the consolidated broadcast zone, which contains all of the devices that can receive broadcast packets. The actual delivery of broadcast packets is also controlled by the Admin Domain and zone enforcement logic. The consolidated broadcast zone is not an actual zone, but is just an abstraction used for explaining the behavior.

- The broadcast zone for AD1 includes member devices “1,1”, “3,1” and “5,1”; however, “3,1” and “5,1” are not members of AD1. Consequently, from the AD1 broadcast zone, only “1,1” is added to the consolidated broadcast zone.
- The broadcast zone for AD2 includes member devices “2,1”, “3,1”, and “4,1”. Even though “2,1” is a member of AD1, it is not a member of AD2 and so is not added to the consolidated broadcast zone.
- Device “3,1” is added to the consolidated broadcast zone because of its membership in the AD2 broadcast zone.

When a switch receives a broadcast packet it forwards the packet only to those devices which are zoned with the sender and are also part of the consolidated broadcast zone.
You can run `zone -validate` on a broadcast zone to check if it has any invalid members that cannot be enforced in the current AD context.

Upgrade and downgrade considerations

If you upgrade from a Fabric OS version earlier than 5.3.0 to Fabric OS 5.3.0 or later, you must rename any existing zones named “broadcast” before you upgrade. The firmware download fails if a pre-5.3.x switch has a zone with the name of “broadcast” in the effective configuration.

When downgrading to a firmware version earlier than Fabric OS 5.3.0, you must remove or disable the broadcast zone. The firmware downgrade fails if a zone with the name of “broadcast” is part of the effective configuration.

High Availability considerations with broadcast zones

If a switch has broadcast zone-capable firmware on the active CP (Fabric OS 5.3.x or later) and broadcast zone-incapable firmware on the standby CP (Fabric OS version earlier than 5.3.0), then you cannot create a broadcast zone because the zoning behavior would not be the same across an HA failover. If the switch failed over, then the broadcast zone would lose its special significance and would be treated as a regular zone.

Loop devices and broadcast zones

Delivery of broadcast packets to individual devices in a loop is not controlled by the switch. So adding loop devices to a broadcast zone does not have any effect. If a loop device is part of a broadcast zone, then all devices in that loop receive broadcast packets.

Best practice: All devices in a single loop should have uniform broadcast capability. If all the devices in the loop can handle broadcast frames, then add the FL_Port to the broadcast zone.

Backward compatibility with pre-5.3.0 switches

In a broadcast zone, you should not include any members connected to switches running firmware versions earlier than Fabric OS 5.3.0. For pre-5.3.0 switches, the “broadcast” zone name does not have any special significance and a broadcast zone appears as a regular zone.

If a broadcast zone has any members that are connected to pre-5.3.0 switches, then those devices are zoned together.

Broadcast packets are checked only for local devices in the fabric. If a remote switch is running pre-5.3.0 firmware, the broadcast zone does not have any effect on devices connected to that remote switch.

The `zone --validate` command can flag devices that are part of a broadcast zone and are connected to a pre-5.3.0 switch. It is strongly recommended that you run `zone --validate` whenever zone configurations are changed or any devices are moved in a fabric.

Broadcast zones and default zoning

The default zoning mode defines the device accessibility behavior if zoning is not implemented or if there is no effective zone configuration. The default zoning mode has two options:

- **All Access**—All devices within the fabric can communicate with all other devices.
- **No Access**—Devices in the fabric cannot access any other device in the fabric.

If a broadcast zone is active, even if it is the only zone in the effective configuration, the default zone setting is not in effect.

If the effective configuration has only a broadcast zone, then the configuration appears as a No Access configuration. To change this configuration to All Access, you must put all the available devices in a regular zone.

See “Activating default zones” on page 403 for additional information about default zoning.
Creating and managing zone aliases

A zone alias is a logical group of ports or WWNs. You can simplify the process of creating zones by first specifying aliases, which eliminates the need for long lists of individual zone member names.

If you are creating a new alias using `aliCreate w, “1,1”,` and a user in another Telnet session executes `cfgEnable` (or `cfgDisable`, or `cfgSave`), the other user’s transaction will abort your transaction and you will receive an error message. Creating a new alias while there is a zone merge taking place might also abort your transaction. For more details about zone merging and zone merge conflicts, see “Adding a new switch or fabric” on page 414.

To create an alias:

1. Connect to the switch and log in as admin.
2. Enter the `aliCreate` command, using the following syntax:
   ```
   alicreate "aliasname", "member[, member...]"
   ```
   The values represent the following:
   - `aliasname`: The name of the zone alias to be created.
   - `member`: A member or list of members to be added to the alias. An alias member can be specified by one or more of the following methods:
     - A domain,port pair.
     - Device node or device port WWN

   3. Enter the `cfgSave` command to save the change to the defined configuration.

      ```
      switch:admin> alicreate "array1", "2,32; 2,33; 2,34; 4,4"
      switch:admin> alicreate "array2", "21:00:00:20:37:0c:66:23; 4,3"
      switch:admin> alicreate "loop1", "4,6"
      switch:admin> cfgsave
      ```

      You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.

      Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

   To add members to an alias:

   1. Connect to the switch and log in as admin.
   2. Enter the `aliAdd` command, using the following syntax:
      ```
      aliadd "aliasname", "member[, member...]"
      ```
      The values represent the following:
      - `aliasname`: The name of the zone alias.
      - `member`: A member or list of members to be added to the alias. An alias member can be specified by one or more of the following methods:
        - A domain,port pair.
        - Device node or device port WWN

   3. Enter the `cfgSave` command to save the change to the defined configuration.

      ```
      switch:admin> aliadd "array1", "1,2"
      switch:admin> aliadd "array2", "21:00:00:20:37:0c:72:51"
      switch:admin> aliadd "loop1", "5,6"
      switch:admin> cfgsave
      ```
You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.

Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

To remove members from an alias:

1. Connect to the switch and log in as admin.
2. Enter the aliRemove command, using the following syntax:
   
   aliRemove "aliasname", "member[; member...]"

   The values represent the following:
   
   aliasname The name of the zone alias.
   member A member or list of members to be removed from the alias. An alias member can be specified by one or more of the following methods:
   
   • A domain,port pair.
   • Device node or device port WWN

3. Enter the cfgSave command to save the change to the defined configuration.

   switch:admin> aliRemove "array1", "1,2"
   switch:admin> aliRemove "array2", "21:00:00:20:37:0c:72:51"
   switch:admin> aliRemove "loop1", "4,6"
   switch:admin> cfgSave

You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.

Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

NOTE: For Fabric OS versions earlier than 4.4.0, when using the aliRemove command, the order in which the members appear in the list is critical. For more information on this command, see the Fabric OS Command Reference.

To delete an alias:

1. Connect to the switch and log in as admin.
2. Enter the aliDelete command, using the following syntax.

   aliDelete "aliasname"

   The value represents the following:
   
   aliasname The name of the zone alias to be deleted.
3. Enter the `cfgSave` command to save the change to the defined configuration.

```
switch:admin> alidelete "array1"
switch:admin> cfgsave
```
You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.

Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

To view an alias in the defined configuration:

1. Connect to the switch and log in as admin.

2. Enter the `aliShow` command, using the following syntax

```
aliShow "pattern"[, mode]
```

The values represent the following:

- **pattern**: A POSIX-style regular expression used to match zone alias names.
- **mode**: Specify 0 to display the contents of the transaction buffer (the contents of the current transaction), or specify 1 to display the contents of the nonvolatile memory. The default value is 0.

The following example shows all zone aliases beginning with “arr”.

```
switch:admin> aliShow "arr*"
alias: array1 21:00:00:20:37:0c:76:8c
alias: array2 21:00:00:20:37:0c:66:23
```

If no parameters are specified, the entire zone database (both the defined and effective configuration) is displayed.

**Creating and maintaining zones**

Before executing `cfgDisable`, `cfgEnable`, or `cfgSave`, execute the `rcsDisabled` command to check whether your fabric has Reliable Commit Service (RCS) enabled (`rcsDisabled=0`). If RCS is disabled (`rcsDisabled=1`), check for older switches in the fabric. After the older switches are upgraded, RCS is enabled by default.

RCS is available on all switches running Fabric OS versions 4.1 and later. RCS guarantees that either all or none of the switches receive the new zone configuration. You should use RCS to secure a reliable propagation of the latest zone configuration. If you use non-RCS mode, you must log in to every switch to monitor the status of the zone configuration.

To create a broadcast zone, use the reserved name “broadcast”. Do not give a regular zone the name of “broadcast”. See “Broadcast zones” on page 395 for additional information.

To create a zone:

1. Connect to the switch and log in as admin.

2. Enter the `zoneCreate` command, using the following syntax:

```
zoneCreate "zonename", "member[; member...]"
```
To create a broadcast zone, use the reserved name “broadcast”.

3. Enter the `cfgSave` command to save the change to the defined configuration.
   ```
   switch:admin> zonecreate "greenzone", "2,32; 2,33; 2,34; 4,4"
   switch:admin> zonecreate "redzone", "21:00:00:20:37:0c:66:23; 4,3"
   switch:admin> zonecreate "broadcast", "1,2; 2,33; 2,34"
   switch:admin> cfgsave
   ```
   You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration.
   Any changes made on the Effective configuration will not take effect until it is re-enabled.
   Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

To add devices (members) to a zone:

1. Connect to the switch and log in as admin.
2. Enter the `zoneAdd` command, using the following syntax:
   ```
   zoneadd "zonename", "member[; member...]"
   ```

The values represent the following:

- **zonename**: The name of the zone to be created.
- **member**: A member or list of members to be added to the zone. A zone member can be specified by one or more of the following methods:
  - A domain,port pair.
  - Device node or device port WWN
  - Zone alias name

3. Enter the `cfgSave` command to save the change to the defined configuration.
   ```
   switch:admin> zoneadd "greenzone", "1,2"
   switch:admin> zoneadd "redzone", "21:00:00:20:37:0c:72:51"
   switch:admin> zoneadd "broadcast", "1,3"
   switch:admin> cfgsave
   ```
   You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration.
   Any changes made on the Effective configuration will not take effect until it is re-enabled.
   Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y
To remove devices (members) from a zone:

1. Connect to the switch and log in as admin.
2. Enter the `zoneremove` command, using the following syntax:
   
   ```
   zoneremove "zonename", "member[; member...]
   ```
   
   The values represent the following:
   
   - `zonename`: The name of the zone to be created.
   - `member`: A member or list of members to be removed from the zone. A zone member can be specified by one or more of the following methods:
     - A `domain,port` pair.
     - Device node or device port WWN
     - Zone alias name

3. Enter the `cfgSave` command to save the change to the defined configuration.
   
   ```
   switch:admin> zoneremove "greenzone", "1,2"
   switch:admin> zoneremove "redzone", "21:00:00:20:37:0c:72:51"
   switch:admin> zoneremove "broadcast", "2,34"
   ```
   
   You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.
   
   Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

To delete a zone:

1. Connect to the switch and log in as admin.
2. Enter the `zoneDelete` command, using the following syntax:
   
   ```
   zonedelete "zonename"
   ```
   
   The value represents the following:
   
   - `zonename`: The name of the zone to be deleted.

3. Enter the `cfgSave` command to save the change to the defined configuration.
   
   ```
   switch:admin> zonedelete "redzone"
   ```
   
   You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.
   
   Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

To view a zone in the defined configuration:

1. Connect to the switch and log in as admin.
2. Enter the `zoneshow` command, using the following syntax:
   
   ```
   zoneshow "pattern"[, mode]
   ```
The values represent the following:

- **pattern**: A POSIX-style regular expression used to match zone names.
- **mode**: Specify 0 to display the contents of the transaction buffer (the contents of the current transaction), or specify 1 to display the contents of the nonvolatile memory. The default value is 0.

The following example shows all zones beginning with A, B, or C:

```
switch:admin> zoneshow "[A-C]*"
zone: Blue_zone 1,1; array1; 1,2; array2
zone: Bobs_zone 4,5; 4,6; 4,7; 4,8; 4,9
```

If no parameters are specified, the entire zone database (both the defined and effective configuration) is displayed.

### Activating default zones

Typically, when you issue the `cfgDisable` command in a large fabric with thousands of devices, the name server indicates to all hosts that they can communicate with each other. In fact, each host can receive an enormous list of PIDs, and ultimately cause other hosts to run out of memory or crash. To ensure that all devices in a fabric do not see each other during a `cfgDisable` operation, you can activate a **default zone**.

A default zone includes all devices in a fabric that are not members of an active zone set. Depending on the configuration, default zones are activated whenever you enter the `cfgDisable` command. Default zones have the following properties:

- Any Nx_Port that is not a member of any zone in the active zone set is a member of the default zone.
- The fabric does not permit members of the default zone to interact with members of any other zone.
- The fabric might not allow members of the default zone to interact with other members of the default zone.

When you activate default zoning, a new zone alias is created in the defined zone configuration and is propagated to the fabric when you type the `cfgSave` command. Then, when you issue the `cfgDisable` command, if the zone alias exists, zoning actually interprets the `cfgDisable` command as a `cfgEnable` command for the default zone. The default zone applies to the entire fabric (regardless of switch model).

**NOTE:** If you want to use Admin Domains, you must set the default zoning mode to No Access prior to setting up the Admin Domains. You cannot change the default zoning mode to All Access if user-specified Admin Domains are present in the fabric.

To activate a default zone:

1. Connect to the switch and log in as admin.
2. Enter the `cfgActvShow` command to view the current zone configuration.
3. Enter the `defZone --noaccess` command, which initiates a transaction (if one is not already in progress) and prevents all Nx_Ports from communicating with each other.
4. Enter either the `cfgSave`, `cfgEnable`, or `cfgDisable` command to commit the change and distribute it to the fabric. The change will not be committed and distributed across the fabric if you do not enter one of these commands.

After setting the default zone access mode to `noaccess`, subsequent use of the `cfgDisable` command performs the equivalent of the `cfgEnable "d_efault_Cmd"` command.

To view the current default zone access mode:

1. Connect to the switch and log in as admin.
2. Enter the `defZone --show` command.
NOTE: If you performed a firmware download of an older release, then the current default zone access state will appear as it did prior to the download. For example, if the default_Cfg was in effect before the download, it will remain in effect afterward.

See the Fabric OS Command Reference for additional information on the defZone command.

Merging zones

Table 88 presents zoning database size limitations for various Fabric OS release versions. The maximum size of a zone database is the upper limit for the defined configuration, and it is determined by the amount of flash memory available for storing the defined configuration.

**Table 88  Zoning database limitations**

<table>
<thead>
<tr>
<th>Fabric OS version</th>
<th>Maximum database size (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.0</td>
<td>64</td>
</tr>
<tr>
<td>2.5.0</td>
<td>64</td>
</tr>
<tr>
<td>2.6.0</td>
<td>96</td>
</tr>
<tr>
<td>3.0.0</td>
<td>128</td>
</tr>
<tr>
<td>3.1.0</td>
<td>96</td>
</tr>
<tr>
<td>3.2.0</td>
<td>256</td>
</tr>
<tr>
<td>4.0.0, 4.1.0, 4.2.0</td>
<td>128</td>
</tr>
<tr>
<td>4.4.0</td>
<td>256</td>
</tr>
<tr>
<td>5.0.1</td>
<td>256</td>
</tr>
<tr>
<td>5.1.0</td>
<td>256</td>
</tr>
<tr>
<td>5.2.0 or later</td>
<td>1024 (see the following note for restrictions)</td>
</tr>
</tbody>
</table>

Before linking two switches together, it is important that you know the zone database limit of adjacent switches. For example, when switches running Fabric OS 3.2, 4.4.0, or 5.1.0 discover that the zone merge database is larger than its pre-determined zone database size limit, they issue a reject notification before symmetrically segmenting their own ends of the ISL, thereby preventing the new switch from joining the fabric.

**NOTE:** Fabric OS 5.2.0 and later support a zoning database size of 1 MB. To support a 1 MB zoning database, the entire fabric must be upgraded to 5.2.0 or later. If any pre-5.2.0 switches are part of the fabric, the maximum zone database size is 256 KB. If the zoning database size exceeds 256 KB, switches not upgraded to Fabric OS 5.2.0 or later are segmented out of the fabric. Use the cfgSize command to display the zoning database size.

Symmetrical segmentation occurs when both ends of an ISL are shut down. Subsequently, no frames are exchanged between those two switches.

Asymmetrical segmentation not only prevents frames from being exchanged between switches, but also causes routing inconsistencies.

The best way to avoid either type of segmentation is to know the zone database size limit of adjacent switches. The following tables provide the expected behavior based on different database sizes after a zone merge is specified.
## Table 89  Resulting database size: 0 to 96K

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Fabric OS 2.6</th>
<th>Fabric OS 3.1</th>
<th>Fabric OS 3.2</th>
<th>Fabric OS 4.0/4.1/4.2</th>
<th>Fabric OS 4.3/4.4.0</th>
<th>Fabric OS 5.0.0/5.0.1/5.1.0</th>
<th>Fabric OS 5.2.0/5.3.0</th>
<th>Fiber Channel Router</th>
<th>XPath OS 7.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric OS 2.6/3.1</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 3.2</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 4.0/4.1/4.2</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 4.4.0</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 5.0.0/5.0.1/5.1.0</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 5.2.0/5.3.0</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fibre Channel Router</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>XPath OS 7.3</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
</tbody>
</table>

## Table 90  Resulting database size: 96K to 128K

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Fabric OS 2.6</th>
<th>Fabric OS 3.1</th>
<th>Fabric OS 3.2</th>
<th>Fabric OS 4.0/4.1/4.2</th>
<th>Fabric OS 4.3/4.4.0</th>
<th>Fabric OS 5.0.0/5.0.1/5.1.0</th>
<th>Fabric OS 5.2.0/5.3.0</th>
<th>Fiber Channel Router</th>
<th>XPath OS 7.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric OS 2.6/3.1</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 3.2</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 4.0/4.1/4.2</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 4.4.0</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 5.0.0/5.0.1</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fabric OS 5.2.0/5.3.0</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Fibre Channel Router</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>XPath 7.3</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
</tr>
<tr>
<td>Receiver Initiator</td>
<td>Fabric OS 2.6</td>
<td>Fabric OS 3.1</td>
<td>Fabric OS 3.2</td>
<td>Fabric OS 4.0/4.1/4.2</td>
<td>Fabric OS 4.3/4.4.0</td>
<td>Fabric OS 5.0.0/5.0.1/5.1.0</td>
<td>Fabric OS 5.2.0/5.3.0</td>
<td>Fibre Channel Router</td>
<td>XPath 7.3</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
<td>-----------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>---------------------</td>
<td>----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Fabric OS 2.6/3.1</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 3.2</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 4.0/4.1/4.2</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 4.4.0</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 5.0.0/5.0.1</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 5.2.0/5.3.0</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
</tr>
</tbody>
</table>

Table 91 Resulting database size: 128K to 256K

<table>
<thead>
<tr>
<th>Receiver Initiator</th>
<th>Fabric OS 2.6</th>
<th>Fabric OS 3.1</th>
<th>Fabric OS 3.2</th>
<th>Fabric OS 4.0/4.1/4.2</th>
<th>Fabric OS 4.3/4.4.0</th>
<th>Fabric OS 5.0.0/5.0.1/5.1.0</th>
<th>Fabric OS 5.2.0/5.3.0</th>
<th>Fibre Channel Router</th>
<th>XPath 7.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric OS 2.6/3.1</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 3.2</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 4.0/4.1/4.2</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 4.4.0</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 5.0.0/5.0.1/5.1.0</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Asymmetric Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Segmen</td>
<td>Segment</td>
<td>Segment</td>
</tr>
<tr>
<td>Fabric OS 5.2.0/5.3.0</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Segment</td>
</tr>
</tbody>
</table>

Table 92 Resulting database size: 256K to 1M
### Table 92  Resulting database size: 256K to 1M (continued)

<table>
<thead>
<tr>
<th>Receiver Initiator</th>
<th>Fabric OS 2.6</th>
<th>Fabric OS 3.1</th>
<th>Fabric OS 3.2</th>
<th>Fabric OS 4.0/v 4.1/ 4.2</th>
<th>Fabric OS 4.3/ 4.4.0</th>
<th>Fabric OS 5.0.0/ 5.0.1/ 5.1.0</th>
<th>Fabric OS 5.2.0/ 5.3.0</th>
<th>Fibre Channel Router</th>
<th>XPath 7.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fibre Channel Router</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Join</td>
<td>Join</td>
<td>Join</td>
<td>Segment</td>
<td>Segment</td>
</tr>
<tr>
<td>XPath 7.3</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
<td>Segment</td>
</tr>
</tbody>
</table>
Creating and modifying zoning configurations

You can store a number of zones in a zoning configuration database. The maximum number of items that can be stored in the zoning configuration database depends on the following criteria:

- Number of switches in the fabric.
- Whether or not interoperability mode is enabled.
- Number of bytes per item. The number of bytes required for an item depends on the specifics of the fabric, but cannot exceed 64 bytes per item.

When enabling a new zone configuration, you must ensure that the size of the configuration does not exceed the minimum size supported by all switches in the fabric. This is particularly important if and when you downgrade to a Fabric OS version that supports a smaller zone database than the current Fabric OS. In this scenario, the zone database in the current Fabric OS would have to be changed to the smaller zone database before the downgrade.

You can use the `cfgSize` command to check both the maximum available size and the currently saved size on all switches. See the Fabric OS Command Reference for details on the `cfgSize` command. If you believe you are approaching the maximum, you can save a partially completed zoning configuration and use the `cfgSize` command to determine the remaining space.

**NOTE:** For Fabric OS 5.3.0 and later, the minimum zoning database size is 4 bytes, even if the zoning database is empty.

For important considerations for managing zoning in a fabric, and more details about the maximum zone database size for each version of the Fabric OS, see “Merging zones” on page 404.

If you create or make changes to a zone configuration, you must enable the configuration for the changes to take effect.

To create a zoning configuration:

1. Connect to the switch and log in as admin.
2. Enter the `cfgCreate` command, using the following syntax:
   ```
   cfgcreate "cfgname", "member[; member...]"
   ```
   The values represent the following:
   - `cfgname`: The name of the zone configuration to be created.
   - `member`: The zone name or list of zone names to be added to the configuration.

3. Enter the `cfgSave` command to save the change to the defined configuration.
   ```
   switch:admin> cfgcreate "NEW_cfg", "redzone; bluezone; greenzone"
   switch:admin> cfgsave
   ```

To add zones (members) to a zoning configuration:

1. Connect to the switch and log in as admin.
2. Enter the `cfgAdd` command, using the following syntax:
   ```
   cfgadd "cfgname", "member[; member...]"
   ```
The values represent the following:

- `cfgname`: The name of the zone configuration.
- `member`: The zone name or list of zone names to be added to the configuration.

3. Enter the `cfgSave` command to save the change to the defined configuration.

```
switch:admin> cfgadd "newcfg", "bluezone"
switch:admin> cfgsave
```

You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.

Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

To remove zones (members) from a zone configuration:

1. Connect to the switch and log in as admin.
2. Enter the `cfgRemove` command, using the following syntax:

   ```
cfgremov "cfgname", "member[; member...]
```

   The values represent the following:

   - `cfgname`: The name of the zone configuration.
   - `member`: The zone name or list of zone names to be removed from the configuration.

3. Enter the `cfgSave` command to save the change to the defined configuration.

```
switch:admin> cfgremov "NEW_cfg", "redzone"
switch:admin> cfgsave
```

You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.

Do you want to save Defined zoning configuration only? (yes, y, no, n): [no] y

To delete a zone configuration:

1. Connect to the switch and log in as admin.
2. Enter the `cfgDelete` command, using the following syntax:

   ```
cfgdelete "cfgname"
```

   The values represent the following:

   - `cfgname`: The name of the defined zone configuration to be deleted.

3. Enter the `cfgSave` command to save the change to the defined configuration.

```
switch:admin> cfgdelete "testcfg"
switch:admin> cfgsave
```

You are about to save the Defined zoning configuration. This action will only save the changes on the Defined configuration. Any changes made on the Effective configuration will not take effect until it is re-enabled.
Do you want to save Defined zoning configuration only? (yes, y, no, n):  
[no]  y

To clear changes to a configuration:

1. Enter the `cfgTransAbort` command.
  When this command is executed, all changes since the last save operation (performed with the `cfgSave` command) are cleared.
  In the following example, assume that the removal of a member from `zone1` was done in error:
  switch:admin> zoneremove "zone1","3,5"
  switch:admin> cfgtransabort

To view all zone configuration information:

If you do not specify an operand when executing the `cfgShow` command to view zone configurations, then all zone configuration information (both defined and effective) displays. If there is an outstanding transaction, then the newly edited zone configuration that has not yet been saved is displayed. If there are no outstanding transactions, then the committed zone configuration displays.

1. Connect to the switch and log in as admin.
2. Enter the `cfgShow` command with no operands.

```
switch:admin> cfgshow
Defined configuration:
  cfg:  USA1    Blue_zone
  cfg:  USA_cfg Red_zone; Blue_zone
  zone:  Blue_zone
    1,1; array1; 1,2; array2
  zone:  Red_zone
    1,0; loop1
alias: array1  21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
alias: array2  21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
alias: loop1   21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
  cfg:  USA_cfg
  zone:  Blue_zone
    1,1
    21:00:00:20:37:0c:76:8c
    21:00:00:20:37:0c:71:02
    1,2
    21:00:00:20:37:0c:76:22
    21:00:00:20:37:0c:76:28
  zone:  Red_zone
    1,0
    21:00:00:20:37:0c:76:85
    21:00:00:20:37:0c:71:df
```

To view selected zone configuration information:

1. Connect to the switch and log in as admin.
2. Enter the `cfgShow` command and specify a pattern.

```
cfgshow "pattern"[, mode]
```

The values represent the following:

- `pattern` A POSIX-style regular expression used to match zone configuration names.
- `mode` Specify 0 to display the contents of the transaction buffer (the contents of the current transaction), or specify 1 to display the contents of the nonvolatile memory. The default value is 0.
For example, to display all zone configurations that start with “Test”:

```
switch:admin> cfgshow "Test*"
cfg:   Test1 Blue_zone
cfg:   Test_cfg Red_zone; Blue_zone
```

To view a configuration in the effective zone database:

1. Connect to the switch and log in as admin.
2. Enter the `cfgActvShow` command.

```
switch:admin> cfgactvshow
Effective configuration:
  cfg:   NEW_cfg
  zone:  Blue_zone
    1,1
    21:00:00:20:37:0C:76:8C
    21:00:00:20:37:0C:71:02
    1,2
    21:00:00:20:37:0C:76:22
    21:00:00:20:37:0C:76:28
  zone:  Red_zone
    1,0
    21:00:00:20:37:0C:76:85
    21:00:00:20:37:0C:71:DF
```

**Maintaining zone objects**

Although you can use the `cfgDelete` command to delete a zone configuration, there is a quicker and easier way to perform the same task with the zone object commands (`zoneObjectExpunge`, `zoneObjectCopy`, and `zoneObjectRename`). You can also copy and rename zone objects. When you copy a zone object, the resulting object has the same type as the original. Deleting a zone object also removes the object from any member lists of other objects. You can rename objects for all zone object types.

To copy a zone object:

1. Connect to the switch and log in as admin.
2. Enter the `cfgShow` command to view the zone configuration objects you want to copy.

```
cfgshow "pattern[, mode]"
```

The values represent the following:

- `pattern` A POSIX-style regular expression used to match zone configuration names.
- `mode` Specify 0 to display the contents of the transaction buffer (the contents of the current transaction), or specify 1 to display the contents of the nonvolatile memory. The default value is 0.

For example, to display all zone configuration objects that start with “Test”:

```
switch:admin> cfgshow "Test*"
cfg:   Test1 Blue_zone
```

3. Enter the `zone --copy` command, specifying the zone configuration objects you want to copy, along with the new object name. Note that zone configuration names are case-sensitive; blank spaces are ignored and it works in any Admin Domain other than AD255.

```
switch:admin> zone --copy "Test1", "US_Test1"
```
4. Enter the \texttt{cfgShow} command to verify the new zone object is present.

\begin{verbatim}
switch:admin> cfgshow "Test*"
cfg: Test1 Blue_zone
cfg: Test_cfg Red_zone; Blue_zone
switch:admin> cfgShow "US_Test1"
cfg: Test1 Blue_zone
cfg: Test_cfg Red_zone; Blue_zone
\end{verbatim}

5. If you want the change preserved when the switch reboots, enter the \texttt{cfgSave} command to save it to nonvolatile (flash) memory.

6. Enter the \texttt{cfgEnable} command for the appropriate zone configuration to make the change effective.

To delete a zone object:

1. Connect to the switch and log in as admin.

2. Enter the \texttt{cfgShow} command to view the zone configuration objects you want to delete.

\begin{verbatim}
switch:admin> cfgShow
Defined configuration:
cfg: USA_cfg Red_zone; White_zone; Blue_zone
zone: Blue_zone
  1,1; array1; 1,2; array2
zone: Red_zone
  1,0; loop1
zone: White_zone
  1,3; 1,4
alias: array1 21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
alias: array2 21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
alias: loop1 21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df

Effective configuration:
cfg: USA_cfg
zone: Blue_zone
  1,1
21:00:00:20:37:0c:76:8c
21:00:00:20:37:0c:71:02
  1,2
21:00:00:20:37:0c:76:22
21:00:00:20:37:0c:76:28
zone: Red_zone
  1,0
21:00:00:20:37:0c:76:85
21:00:00:20:37:0c:71:df
\end{verbatim}

3. Enter the \texttt{zone --expunge} command to delete the zone object. Note that zone configuration names are case-sensitive; blank spaces are ignored and it works in any Admin Domain other than AD255.

\begin{verbatim}
switch:admin> zone --expunge "White_zone"
\end{verbatim}

4. Enter the \texttt{cfgShow} command to verify the deleted zone object is no longer present.

5. If you want the change preserved when the switch reboots, enter the \texttt{cfgSave} command to save it to nonvolatile (flash) memory.

6. Enter the \texttt{cfgEnable} command for the appropriate zone configuration to make the change effective.
To rename a zone object:

1. Connect to the switch and log in as admin.
2. Enter the `cfgShow` command to view the zone configuration objects you want to rename.
   ```
   switch:admin> cfgShow
   Defined configuration:
   cfg: USA_cfg Red_zone; White_zone; Blue_zone
   zone: Blue_zone
       1,1; array1; 1,2; array2
   zone: Red_zone
       1,0; loop1
   zone: White_zone
       1,3; 1,4
   alias: array1 21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
   alias: array2 21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
   alias: loop1 21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df
   ```
3. Enter the `zoneObjectRename` command to rename zone configuration objects. Note that zone configuration names are case-sensitive; blank spaces are ignored and it works in any Admin Domain other than AD255.
   ```
   switch:admin> zoneObjectRename "White_zone", "Red_zone"
   ```
4. Enter the `cfgShow` command to verify the renamed zone object is present.
5. If you want the change preserved when the switch reboots, enter the `cfgSave` command to save it to nonvolatile (flash) memory.
6. Enter the `cfgEnable` command for the appropriate zone configuration to make the change effective.

To validate a zone:

1. Connect to the switch and log in as admin.
2. Enter the `cfgShow` command to view the zone configuration objects you want to validate.
   ```
   switch:admin> cfgShow
   Defined configuration:
   cfg: USA_cfg Red_zone; White_zone; Blue_zone
   zone: Blue_zone
       1,1; array1; 1,2; array2
   zone: Red_zone
       1,0; loop1
   zone: White_zone
       1,3; 1,4
   alias: array1 21:00:00:20:37:0c:76:8c; 21:00:00:20:37:0c:71:02
   alias: array2 21:00:00:20:37:0c:76:22; 21:00:00:20:37:0c:76:28
   alias: loop1 21:00:00:20:37:0c:76:85; 21:00:00:20:37:0c:71:df
   ```
3. Enter the `zone --validate` command to list all zone members that are not part of the current zone enforcement table. Note that zone configuration names are case-sensitive; blank spaces are ignored.
   ```
   switch:admin> zone --validate "White_zone"
   ```
4. To validate all zones in the zone database in the defined configuration.

```
switch:admin> sw5:root> zone --validate -m 1
Defined configuration:
cfg:  cfg1    zone1
cfg:  cfg2    zone1; zone2
zone: zone1   1,1; ali1
zone: zone2   1,1; ali2
alias: ali1   10:00:00:05:1e:35:81:7f*; 10:00:00:05:1e:35:81:7d*
alias: ali2   10:00:00:05:1e:35:81:09*; 10:00:00:05:1e:35:81:88*

------------------------------------
~ - Invalid configuration
* - Member does not exist
```

The mode flag -m can be used to specify the zone database location. Supported mode flag values are:

- 0 — zone database from the current transaction buffer
- 1 — zone database stored from the persistent storage
- 2 — currently effective zone database.

If no mode options are given, the validated output of all three buffers would be shown.

If the -f option is specified, all the zone members that are not enforceable would be expunged in the transaction buffer. This pruning operation would always happen on the transaction and defined buffers. You cannot specify a mode option or specify a zone object as an argument with the -f option. This mode flag should be used after the zone has been validated.

For more details about the `zone`, `cfgShow`, `cfgEnable`, and `cfgSave` commands, see the Fabric OS Command Reference.

Managing zoning configurations in a fabric

You can add, delete, or remove individual elements in an existing zone configuration to create an appropriate configuration for your SAN environment. After the changes have been made, save the configuration to ensure the configuration is permanently saved in the switch and that the configuration is replicated throughout the fabric.

The switch configuration file can also be uploaded to the host for archiving and it can be downloaded from the host to a switch in the fabric. See “Backing up a configuration” on page 131, “Restoring a configuration” on page 134, or the `configUpload` and `configDownload` commands in the Fabric OS Command Reference.

Adding a new switch or fabric

When a new switch is added to the fabric, it automatically takes on the zone configuration information from the fabric. Use the `cfgActvShow` command to verify the zoning information is the same on each switch in the fabric.

If you are adding a switch that is already configured for zoning, use the `cfgClear` and `cfgSave` commands (or use `cfgClear` and `cfgDisable` if there is an effective configuration) before connecting it to the zoned fabric.

Adding a new fabric that has no zone configuration information to an existing fabric is very similar to adding a new switch. All switches in the new fabric inherit the zoning configuration data. If a zone configuration is in effect, then the same configuration becomes the enabled configuration. The `cfgActvShow` command will display the same information on all switches in the newly formed fabric.
Before the new fabric can merge successfully, it must pass the following criteria:

- **Before merging zones**
  To facilitate merging, check the following before merging switches or fabrics:
  - **Zoning licenses**: All switches must have a Zoning license enabled.
  - **Native operating mode**: All switches must be in the native operating mode.
  - **Secure Fabric OS**: The switch being merged into the existing fabric must **not** have Secure Fabric OS enabled.
    
    If Secure Fabric OS is enabled on one switch, it must be enabled on all switches in the fabric; however, Secure Fabric OS is not supported in Fabric OS 6.0.0 or later.
  - **Default Zone**: The switch being merged into the existing fabric should be configured with the same default zone mode as the existing switches.

- **Merging and segmentation**
  The fabric is checked for segmentation during power-up or when a switch is disabled or enabled, or when a new switch is added.

  The database is the zone configuration database. This is the data displayed as the “defined configuration” in the `cfgShow` command. It is stored in nonvolatile memory by the `cfgSave` command. This database is a replicated database, which means that all switches in the fabric will have a copy of this database. When a change is made to the defined configuration, the switch where the changes were made must close its transaction for the change to be propagated throughout the fabric.

  If you have implemented default zoning you must set the switch you are adding into the fabric to the same default zone mode setting as the rest of the fabric to avoid segmentation.

- **Merging rules**
  Observe these rules when merging zones:
  - **Local and adjacent configurations**: If the local and adjacent zone database configurations are the same, they will remain unchanged after the merge.
  - **Effective configurations**: If there is an effective configuration between two switches, the effective zone configurations must match.
  - **Zone object naming**: If a zoning object has the same name in both the local and adjacent defined configurations, the object types and member lists must match. When comparing member lists, the content and order of the members are important.
  - **Objects in adjacent configurations**: If a zoning object appears in an adjacent defined configuration, but not in the local defined configuration, the zoning object is added to the local defined configuration. The modified zone database must fit in the nonvolatile memory area allotted for the zone database.
  - **Local configuration modification**: If a local defined configuration is modified because of a merge, the new zone database is propagated to other the switches within the merge request.

- **Merging Two Fabrics**
  Both fabrics have identical zones and configurations enabled, including the default zone mode. The two fabrics will join to make one larger fabric with the same zone configuration across the newly created fabric.

  If the two fabrics have different zoning configurations, they will be merged. If the two fabrics cannot join, the ISL between the switches will segment.

- **Merge Conflicts**
  When a merge conflict is present, a merge will not take place and the ISL will segment. Use the `switchShow` or `errLogShow` commands to obtain additional information about possible merge conflicts, because many non-zone related configuration parameters can cause conflicts.

  If the fabrics have different zone configuration data, the system attempts to merge the two sets of zone configuration data. If the zones cannot merge, the ISL will be segmented.
A merge is not possible if any of the following conditions exist:

- **Configuration mismatch**: Zoning is enabled in both fabrics and the zone configurations that are enabled are different in each fabric.
- **Type mismatch**: The name of a zone object in one fabric is used for a different type of zone object in the other fabric.
- **Content mismatch**: The definition of a zone object in one fabric is different from the definition of zone object with the same name in the other fabric.
- **Zone Database Size**: If the zone database size exceeds the maximum limit of another switch.

**NOTE:** If the zoneset members on two switches are not listed in the same order, the configuration is considered a mismatch, resulting in the switches being segmented from the fabric. For example: `cfg1 = z1; z2` is different from `cfg1 = z2; z1`, even though members of the configuration are the same. If zoneset members on two switches have the same names defined in the configuration, make sure zoneset members are listed in the same order.

### Splitting a fabric

If the connections between two fabrics are no longer available, the fabric will segment into two separate fabrics. Each new fabric will retain the same zone configuration.

If the connections between two fabrics are replaced and no changes have been made to the zone configuration in either of the two fabrics, then the two fabrics will merge back into one single fabric. If any changes that cause a conflict have been made to either zone configuration, then the fabrics might segment.

### Using zoning to administer security

Zones provide controlled access to fabric segments and establish barriers between operating environments. They isolate systems with different uses, protecting individual systems in a heterogeneous environment; for example, when zoning is in secure mode, no merge operations occur.

Advanced Zoning is configured on the primary Fabric Configuration Server (FCS). The primary FCS switch makes zoning changes and other security-related changes. The primary FCS switch also distributes zoning to all other switches in the secure fabric. All existing interfaces can be used to administer zoning (depending on the policies; see the Secure Fabric OS Administrator’s Guide for information about security policies).

You must perform zone management operations from the primary FCS switch using a zone management interface, such as Telnet or Advanced Web Tools. You can alter a zoning database, provided you are connected to the primary FCS switch.

When two secure fabrics join, the traditional zoning merge does not occur. Instead, a zoning database is downloaded from the primary FCS switch of the merged secure fabric. When E_Ports are active between two switches, the name of the FCS server and a zoning policy set version identifier are exchanged between the switches. If the views of the two secure fabrics are the same, the fabric’s primary FCS server downloads the zoning database and security policy sets to each switch in the fabric. If there is a view conflict, the E_Ports are segmented due to incompatible security data.

As part of zoning architecture, you must determine which of the two basic zoning architectures (hard or soft) works best for your fabric. With time and planning, the basic hard zone configuration works for most sites.

### Resolving zone conflicts

Zone conflicts can be resolved by saving a configuration file with the `configUpload` command, examining the zoning information in the file, and performing a cut and paste operation so that the configuration information matches in the fabrics being merged.

After examining the configuration file, you can choose to resolve zone conflicts by using the `cfgClear` command followed by the `cfgDisable` command on the incorrectly configured segmented fabric, followed by a `portDisable/portEnable` command on one of the ISL ports that connects the fabrics. This will cause a merge, making the fabric consistent with the correct configuration.
IMPORTANT: Use caution using the `cfgClear` command because it deletes the defined configuration.
21 Configuring and monitoring FCIP extension services

This chapter describes the FCIP concepts, configuration procedures, and tools and procedures for monitoring network performance. Commands described in this chapter require Admin or root user access. See the Fabric OS Command Reference for detailed information on command syntax.

FCIP services licensing

Most of the FCIP extension services described in this chapter require the High Performance Extension over FCIP/FC license. Use the licenseShow command to verify the license is present on the hardware used on both ends the FCIP tunnel. For details on obtaining and installing licensed features, see “Acquiring licensed features” on page 33.
Platforms that support SAN extension over IP

Fabric OS supports SAN extension between 400 Multi-protocol Routers or between FR4-18i blades installed on 4/256 SAN Directors or DC SAN Backbone Directors. The 400 Multi-protocol Router and FR4-18i blade integrate sixteen physical Fibre Channel ports and two physical GbE ports as illustrated in Figure 37 and Figure 38.

**Figure 37** FR4-18i port numbering

**Figure 38** 400 Multi-protocol Router port numbering

**NOTE:** The FCIP Tunneling Service for the 400 Multi-protocol Router and FR4-18i blade is not compatible with the XPath FCIP service; nor is it compatible with any other vendor’s implementation.
FCIP concepts

Fibre Channel over IP (FCIP) enables you to connect Fibre Channel SANs over IP-based networks. 400 Multi-protocol Router and FR4-18i blades use FCIP to encapsulate Fibre Channel frames within IP frames that can be sent over an IP network to a partner 400 Multi-protocol Router or FR4-18i blade. When the IP packets are received, the Fibre Channel frames are reconstructed. The Fibre Channel fabric and all Fibre Channel targets and initiators are unaware of the presence of the IP network.

Virtual ports and FCIP tunnels

Each FR4-18i and 400 Multi-protocol Router platform presents sixteen FC ports and sixteen virtual ports. Each GbE interface can support up to 8 FCIP Tunnels which are represented as 8 virtual ports on ge0 and 8 virtual ports on ge1. The mapping of Tunnels on ge0 and ge1 to virtual port numbers are represented in Table 93.

<table>
<thead>
<tr>
<th>GbE port</th>
<th>Tunnels</th>
<th>Virtual ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>ge0</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>23</td>
</tr>
<tr>
<td>ge1</td>
<td>0</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>29</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>31</td>
</tr>
</tbody>
</table>

Virtual port types

Virtual ports may be defined as VE_Ports or VEX_Ports.

**VE_Ports**

VE_Ports (virtual E_Ports) are used to create interswitch links (ISLs) through an FCIP tunnel. If VE_Ports are used on both ends of an FCIP tunnel, the fabrics connected by the tunnel are merged.

**VEX_Port**

A VEX_Port enables FC-FC Routing Service functionality over an FCIP tunnel. VEX_Ports enable interfabric links (IFLs). If a VEX_Port on one end of an FCIP tunnel, the fabrics connected by the tunnel are not merged. The other end of the tunnel must be defined as a VE_Port. VEX_Ports are not used in pairs.

Figure 39 illustrates a portion of a Fibre Channel network that uses FCIP ISLs (VE_Ports connected over the IP WAN network) to join the office and data center SANs into a single larger SAN.
Compression

Data compression can be enabled or disabled on FCIP tunnels. The default setting is to disable compression.

Traffic shaping

Traffic can be shaped by establishing a rate limit per tunnel. A committed rate can be assigned to a port that guarantees a fixed amount of bandwidth. The committed rate setting insures that a FCIP tunnel will operate at a specific fixed rate (given enough FC traffic to consume it). If too little committed rate is defined, the FCIP tunnel would be limited to that rate and performance could be limited.

QoS concepts and implementation over FCIP

Quality of Service (QoS) refers to policies for handling differences in data traffic. These policies are based on data characteristics and delivery requirements. For example, ordinary data traffic is tolerant of delays and dropped packets, but voice and video data are not. QoS policies provide a framework for accommodating these differences in data as it passes through a network.

FOS versions 6.0.0 and higher provide for Fibre Channel QoS through internal QoS priorities. Those priorities can be mapped to TCP/IP network priorities. There are two options for TCP/IP network based QoS:

- Layer three DiffServ code Points (DSCP).
- VLAN tagging and Layer two class of service (L2CoS).
Layer three DiffServ Code Points (DSCP)

Layer three class of service DiffServ Code Points (DSCP) refers to a specific implementation for establishing QoS policies as defined by RFC2475. DSCP uses six bits of the Type of Service (TOS) field in the IP header to establish up to 64 different values to associate with data traffic priority.

DSCP settings are useful only if IP routers are configured to enforce QoS policies uniformly within the network. IP routers use the DSCP value as an index into a Per Hop Behavior (PHB) table. Control connections and data connections may be configured with different DSCP values. Before configuring DSCP settings, determine if the IP network you are using implements PHB, and consult with the network administrator to determine the appropriate DSCP values.

VLAN tagging and layer two class of service (L2CoS)

Devices in physical LANs are constrained by LAN boundaries. They are usually in close proximity to each other, and share the same broadcast/multicast domain. Physical LANs often contain devices and applications that have no logical relationship. Also, when logically related devices and applications reside in separate LAN domains, they must be routed from one domain to the other.

A VLAN is a virtual LAN network. A VLAN may reside within a single physical network, or it may span several physical networks. Related devices and applications that are separated by physical LAN boundaries can reside in the same VLAN. Also, a large physical network can be broken down into smaller VLANs. VLAN traffic is routed using 802.1Q compliant tags within an Ethernet frame. The tag includes a unique VLAN ID, and Class of Service (CoS) priority bits. The CoS priority scheme (sometimes called Layer two Class of Service, or L2CoS), uses only the upper three bits of the TOS field, allowing eight priorities.

When both DSCP and L2CoS are used

If an FCIP tunnel is not VLAN tagged, only DSCP is relevant. If the FCIP tunnel is VLAN tagged, both DSCP and L2CoS are relevant, unless the VLAN is end-to-end, with no intermediate hops in the IP network. Table 94 shows the default mapping of DSCP priorities to L2Cos priorities per tunnel ID. This may be helpful when consulting with the network administrator. These values may be modified per FCIP tunnel.

Table 94  Default Mapping of DSCP priorities to L2Cos Priorities

<table>
<thead>
<tr>
<th>Virtual Circuit (VC)</th>
<th>DSCP priority/bits</th>
<th>L2CoS priority/bits</th>
<th>Assigned to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>46 / 101110</td>
<td>7 / 111</td>
<td>Class F</td>
</tr>
<tr>
<td>1</td>
<td>7 / 000111</td>
<td>1 / 001</td>
<td>Medium QoS</td>
</tr>
<tr>
<td>2</td>
<td>11 / 001011</td>
<td>3 / 011</td>
<td>Medium QoS</td>
</tr>
<tr>
<td>3</td>
<td>15 / 001111</td>
<td>3 / 011</td>
<td>Medium QoS</td>
</tr>
<tr>
<td>4</td>
<td>19 / 010011</td>
<td>3 / 011</td>
<td>Medium QoS</td>
</tr>
<tr>
<td>5</td>
<td>23 / 010111</td>
<td>3 / 011</td>
<td>Medium QoS</td>
</tr>
<tr>
<td>6</td>
<td>27 / 011011</td>
<td>0 / 000</td>
<td>Class 3 Multicast</td>
</tr>
<tr>
<td>7</td>
<td>31 / 011111</td>
<td>0 / 000</td>
<td>Broadcast/Multicast</td>
</tr>
<tr>
<td>8</td>
<td>35 / 100011</td>
<td>0 / 000</td>
<td>Low Qos</td>
</tr>
<tr>
<td>9</td>
<td>39 / 100111</td>
<td>0 / 000</td>
<td>Low Qos</td>
</tr>
<tr>
<td>10</td>
<td>43 / 101011</td>
<td>4 / 100</td>
<td>High QoS</td>
</tr>
<tr>
<td>11</td>
<td>47 / 101111</td>
<td>4 / 100</td>
<td>High QoS</td>
</tr>
<tr>
<td>12</td>
<td>51 / 110011</td>
<td>4 / 100</td>
<td>High QoS</td>
</tr>
<tr>
<td>13</td>
<td>55 / 110111</td>
<td>4 / 100</td>
<td>High QoS</td>
</tr>
<tr>
<td>14</td>
<td>59 / 111011</td>
<td>4 / 100</td>
<td>High QoS</td>
</tr>
<tr>
<td>15</td>
<td>63 / 111111</td>
<td>0 / 000</td>
<td>-</td>
</tr>
</tbody>
</table>
IPSec concepts and implementation over FCIP

Internet Protocol security (IPSec) uses cryptographic security to ensure private, secure communications over Internet Protocol networks. IPSec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. It helps secure your SAN against network-based attacks from untrusted computers, attacks that can result in the denial-of-service of applications, services, or the network, data corruption, and data and user credential theft. By default, when creating an FCIP tunnel, IPSec is disabled.

Used to provide greater security in tunneling on an FR4-18i blade or a 400 Multi-protocol Router, the IPSec feature does not require you to configure separate security for each application that uses TCP/IP. When configuring for IPSec, however, you must ensure that there is an FR4-18i blade or a 400 Multi-protocol Router at each end of the FCIP tunnel. IPSec works on FCIP tunnels with or without IP compression (IPComp), FCIP fastwrite, and tape pipelining.

IPSec requires an IPSec license in addition to the High-Performance Extension over FCIP/FC license.

IPSec uses some terms that you should be familiar with before beginning your configuration. These are standardized terms, but are included here for your convenience.

Table 95  IPSec terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard. FIPS 197 endorses the Rijndael encryption algorithm as the approved AES for use by US Government organizations and others to protect sensitive information. It replaces DES as the encryption standard.</td>
</tr>
<tr>
<td>AES-XCBC</td>
<td>Cipher Block Chaining. A key-dependent one-way hash function (MAC) used with AES in conjunction with the Cipher-Block-Chaining mode of operation, suitable for securing messages of varying lengths, such as IP datagrams.</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header - like ESP, AH provides data integrity, data source authentication, and protection against replay attacks but does not provide confidentiality.</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard is the older encryption algorithm that uses a 56-bit key to encrypt blocks of 64-bit plain text. Because of the relatively shorter key length, it is not a secured algorithm and no longer approved for Federal use.</td>
</tr>
<tr>
<td>3DES</td>
<td>Triple DES is a more secure variant of DES. It uses three different 56-bit keys to encrypt blocks of 64-bit plain text. The algorithm is FIPS-approved for use by Federal agencies.</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload is the IPSec protocol that provides confidentiality, data integrity and data source authentication of IP packets, and protection against replay attacks.</td>
</tr>
<tr>
<td>IKE</td>
<td>IKE stands for Internet Key Exchange. IKE is defined in RFC 2407, RFC 2408 and RFC 2409. IKEv2 is defined in RFC 4306. IKE uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived, and communicating parties are authenticated. The IKE protocol creates a security association (SA) for both parties.</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5, like SHA-1, is a popular one-way hash function used for authentication and data integrity.</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm, like MD5, is a popular one-way hash function used for authentication and data integrity.</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code is a key-dependent, one-way hash function used for generating and verifying authentication data.</td>
</tr>
</tbody>
</table>
The following limitations apply to using IPSec:

- IPv6, NAT, and AH are not supported.
- You can only create a single secure tunnel on a port; you cannot create a nonsecure tunnel on the same port as a secure tunnel.
- IPSec-specific statistics are not supported.
- To change the configuration of a secure tunnel, you must delete the tunnel and recreate it.
- Jumbo frames are not supported for IPSec.
- There is no RAS message support for IPSec.
- Only a single route is supported on an interface with a secure tunnel.
- IPSec can only be configured on IP V4 based tunnels. Secure tunnels cannot be created on a 400 Multi-protocol Router or FR4-18i blade if any IP V6 addresses are defined on either ge0 or ge1.
- Secure Tunnels cannot be defined with VLAN Tagged connections.

Options for enhancing tape write I/O performance

There are two options available for enhancing open systems SCSI tape write I/O performance.

- FCIP fastwrite and tape pipelining.
- FC fastwrite.

FCIP fastwrite and tape pipelining are implemented together. FC fastwrite is an FC-FC routing alternative that disables the local Ethernet ports (ge0 and ge1), making it impossible to configure FCIP fastwrite and tape pipelining and FC fastwrite on the same 400 Multi-protocol Router or FR4-18i blade. Refer to “FC fastwrite concepts” on page 462 for information about FC fastwrite.

FC fastwrite flows may be routed to another 400 Multi-protocol Router or FR4-18i blade on the FC network. This 400 Multi-protocol Router or FR4-18i blade may have active FCIP tunnels over an IP network. FC fastwrite flows may be passed through the FCIP tunnel, but only if the FCIP fastwrite option is disabled on the tunnel.

FCIP fastwrite and tape pipelining

When the FCIP link is the slowest part of the network, consider using FCIP fastwrite and tape write tape pipelining. Supported only in Fabric OS 5.2.x and later, FCIP fastwrite and tape pipelining are two features that provide accelerated speeds for write I/O over FCIP tunnels in some configurations:

- FCIP fastwrite accelerates the SCSI write I/Os over FCIP.
- Tape pipelining accelerates SCSI write I/Os to sequential devices (such as tape drives) over FCIP, which reduces the number of round-trip times needed to complete the I/O over the IP network and speeds up the process. To use tape pipelining, you must also enable fastwrite.
- Both sides of an FCIP tunnel must have matching configurations for these features to work.

FCIP fastwrite and tape pipelining are enabled by turning them on during the tunnel configuration process. They are enabled on a per-FCIP tunnel basis. See “Configuring FCIP tunnels” on page 438 for details.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMAC</td>
<td>A stronger MAC because it is a keyed hash inside a keyed hash.</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association is the collection of security parameters and authenticated keys that are negotiated between IPSec peers.</td>
</tr>
</tbody>
</table>
Constraints for FCIP fastwrite and tape pipelining

Consider the constraints described in Table 96 when configuring tunnels to use either of these features.

Table 96  Using FCIP fastwrite and tape pipelining

<table>
<thead>
<tr>
<th>FCIP fastwrite</th>
<th>Tape pipelining</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each GbE port supports up to 2048 simultaneous accelerated exchanges, which means a total of 2048 simultaneous exchanges combined for fastwrite and tape pipelining.</td>
<td>Each GbE port supports up to 2048 simultaneous accelerated exchanges, which means a total of 2048 simultaneous exchanges combined for fastwrite and tape pipelining.</td>
</tr>
<tr>
<td>Does not affect FICON traffic</td>
<td>Does not affect FICON traffic</td>
</tr>
<tr>
<td>FCIP fastwrite and FC fastwrite are mutually exclusive.</td>
<td>Tape pipelining uses FCIP fastwrite, not FC fastwrite.</td>
</tr>
<tr>
<td>Does not support multiple equal-cost path configurations (see “FCIP fastwrite/tape pipelining configurations” on page 426).</td>
<td>Does not support multiple equal-cost path configurations or multiple non-equal-cost path configurations (see “FCIP fastwrite/tape pipelining configurations” on page 426).</td>
</tr>
<tr>
<td>Class 3 traffic is accelerated with fastwrite.</td>
<td>Class 3 traffic is accelerated between host and sequential device.</td>
</tr>
<tr>
<td>With sequential devices (tape drives), there are 1024 initiator-tape (IT) pairs per GbE port, but 2048 initiator-tape-LUN (ITL) pairs per GbE port. The ITL pairs are shared among the IT pairs. For example: Two ITL pairs for each IT pair as long as the target has two LUNs. If a target has 32 LUNs, 32 ITL pairs for IT pairs. In this case, only 64 IT pairs are associated with ITL pairs. The rest of the IT pairs are not associated to any ITL pairs, so no tape pipelining is performed for those pairs. By default, only fastwrite-based acceleration is performed on the unassociated pairs.</td>
<td></td>
</tr>
<tr>
<td>Does not support multiple non-equal-cost path between host and sequential device</td>
<td></td>
</tr>
</tbody>
</table>

FCIP fastwrite/tape pipelining configurations

To help understand the supported configurations, consider the configurations shown in the two figures below. In both cases, there are no multiple equal-cost paths. In the first figure, there is a single tunnel with fastwrite and tape pipelining enabled. In the second figure, there are multiple tunnels, but none of them create a multiple equal-cost path.
Unsupported configurations

The following configurations are not supported with fastwrite and tape pipelining. These configurations use multiple equal-cost paths.
FICON emulation concepts

FICON emulation supports FICON traffic over IP WANs using FCIP as the underlying protocol. FICON emulation can be extended to support performance enhancements for specific applications.

Figure 42 Unsupported configurations with fastwrite and tape pipelining
XRC emulation

The eXtended Remote Copy (XRC) application is a DASD application that implements disk mirroring, as supported by the disk hardware architecture and a host software component called System Data Mover (SDM). The primary volume and the secondary mirrored volume may be geographically distant across an IP WAN. The latency introduced by greater distance creates delays in anticipated responses to certain commands. The FICON pacing mechanism may interpret delays as an indication of a large data transfer that could monopolize a shared resource, and react by throttling the I/O. XRC emulation provides local responses to remote hosts, eliminating distance related delays. A FICON XRC Emulation License is required to enable XRC Emulation.

Tape write pipelining

FICON tape write pipelining improves performance for a variety of applications when writing to tape over extended distances. FICON tape write pipelining locally acknowledges write data records, enabling the host to generate more records while previous records are in transit across the IP WAN. If exception status is received from the device, the writing of data and emulation is terminated. The FICON Tape Emulation License is required to enable FICON tape write pipelining.

Tape read pipelining

FICON tape read pipelining improves performance for certain applications when reading from FICON tape over extended distances. FICON tape read pipelining reads data from tape directly from the tape device. Reading of tape continues until a threshold is reached. The buffered data is forwarded to the host in response to requests from the host. When the host sends the status accept frame indicating that the data was delivered, the read processing on the device side credits the pipeline and requests more data from the tape. If exception status is received from the device, the reading of data and emulation is terminated. The FICON Tape Emulation License is required to enable FICON tape read pipelining.

Device level acknowledgment

This feature generates device level acknowledgment (Acks) for non-emulated sequences when an exchange is left open until status acceptance occurs. This can reduce the time it takes to execute some non-emulated channel programs by eliminating one link round trip delay. This feature should be enabled whenever FICON Tape or FICON XRC emulation is enabled.

TIN/TIR emulation

This feature enhances recovery when a TIN/TIR exchange occurs as part of a channel recovery operation during tape emulation. This feature should be enabled whenever FICON Tape or FICON XRC emulation is enabled.

Read block ID emulation

This feature permits FICON write channel programs containing embedded read block ID commands (CCWs) with a byte count of exactly four bytes to be processed as emulated commands during write emulation processes.

FTRACE concepts

FTRACE is a support tool that can be used in a manner similar to that of a channel protocol analyzer. FTRACE enables troubleshooting of problems using a Telnet session rather than sending an analyzer or technical support personnel to the site. FTRACE record events that occur on the FC interface, including user defined messages and events. FTRACE includes the ability to freeze traces on certain events, and to retain the trace information for future examination.
FCIP services configuration guidelines

There are multiple configuration requirements and options associated with FCIP services. The following general guidelines may be helpful. The steps are presented in an order that minimizes the number of times ports need to be disabled and enabled. In practice, the steps do not have to be taken in this order.

1. Determine if you are implementing IPSec.
   IPSec configuration may be done at any time, but defining IPSec policies first ensures that they will be available when FCIP tunnels are configured. Refer to “Configuring IPSec” on page 431 for specific instructions.

2. Determine which FCIP tunnel you want to configure.
   Each FCIP tunnel is associated with a specific virtual port, and a specific Ethernet port, as shown in Table 93. For example, if you want to configure FCIP tunnel 0, you need to configure virtual port 16, and define an IP interface and one or more IP routes over Ge0.

3. Persistently disable the virtual ports before you configure them.
   Ports on a new 400 Multi-protocol Router or FR4-18i blade are persistently disabled by default. On a 400 Multi-protocol Router or FR4-18i blade that has already been installed and configured, check the EX port status using the portcfgshow command, and persistently disable the ports using the portcfgpersistentdisable command before you configure them. Refer to “Persistently disabling ports” on page 435 for a description.

4. The Ethernet port associated with the tunnel should also be disabled. Before disabling an Ethernet port, be sure there are no other tunnels active on the port. If there are, disabling the port will disable the tunnel or tunnels.

5. Determine if any of the Virtual ports should be VEX ports, and configure them using the portcfgvexport command. Refer to “Configuring VEX ports” on page 435 for specific instructions.

6. Create an IP interface using the portcfg ipif command. Refer to “Configuring IP interfaces and IP routes” on page 436 for specific instructions.

7. Create one or more IP routes using the portcfg iproute command. Refer to “Configuring IP interfaces and IP routes” on page 436 for specific instructions.

8. If you are implementing VLAN tagging, create a static ARP entry for the IP interface using the portcfg arp command. Refer to “Configuring IP interfaces and IP routes” on page 436 for specific instructions.

9. Test the IP connection using the portcmd --ping command. Refer to “Configuring IP interfaces and IP routes” on page 436 for specific instructions.

10. Create an FCIP tunnel using the portcfg fciptunnel command. Refer to “Configuring FCIP tunnels” on page 438 for specific instructions.

11. If you are implementing FICON emulation, configure FICON emulation using the portcfg ficon command. Refer to “Configuring FICON emulation” on page 439 for specific instructions.

12. If you are implementing FTRACE, configure FTRACE using the portcfg ftrace command. Refer to “Configuring FTRACE” on page 441 for specific instructions.

13. Check the configuration using the portshow fciptunnel command.

14. Persistently enable the ports using the portpersistentenable command.

15. Create a matching configuration on the 400 Multi-protocol Router or FR4-18i blade at the other end of the tunnel.

Checklist for configuring FCIP links

Table 97 can be used as a checklist for creating FCIP links.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure IPSec policies (optional).</td>
<td>policy - -create</td>
</tr>
<tr>
<td>2. Persistently disable ports.</td>
<td>portcfgpersistentdisable</td>
</tr>
</tbody>
</table>
Configuring IPSec

IPSec requires predefined configurations for IKE and IPSec. You can enable IPSec only when these configurations are well-defined and properly created in advance.

The following describes the sequence of events that invokes the IPSec protocol.

1. Traffic from an IPSec peer with the lower local IP address initiates the IKE negotiation process.
2. IKE negotiates SAs and authenticates IPSec peers, and sets up a secure channel for negotiation of phase 2 (IPSec) SAs.
3. IKE negotiates SA parameters, setting up matching SAs in the peers. Some of the negotiated SA parameters include encryption and authentication algorithms, Diffie-Hellman key exchange, and SA lifetimes.
4. Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. IPSec tunnel termination. SA lifetimes terminate through deletion or by timing out.

All of these steps require that the correct policies have been created. Because policy creation is an independent procedure from FCIP tunnel creation, you must know which IPSec configurations have been created. This ensures that you choose the correct configurations when you enable an IPSec tunnel.

The first step to configuring IPSec is to create a policy for IKE and a policy for IPSec. Once the policies have been created, you assign the policies when creating the FCIP tunnel.

IKE negotiates SA parameters and authenticates the peer using the preshared key authentication method. Once the 2 phases of the negotiation are completed successfully, the actual encrypted data transfer can begin.
IPSec policies are managed using the `policy` command.

You can configure up to 32 IKE and 32 IPSec policies. Policies cannot be modified; they must be deleted and recreated in order to change the parameters. You can delete and recreate any policy as long as the policy is not being used by an active FCIP tunnel.

Each FCIP tunnel is configured separately and may have the same or different IKE and IPSec policies as any other tunnel. Only one IPSec tunnel can be configured for each GbE port.

**IPSec parameters**

When creating policies, the parameters listed in Table 98 are fixed and cannot be modified:

**Table 98  Fixed policy parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Fixed Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE negotiation protocol</td>
<td>Main mode</td>
</tr>
<tr>
<td>ESP</td>
<td>Tunnel mode</td>
</tr>
<tr>
<td>IKE negotiation authentication method</td>
<td>Preshared key</td>
</tr>
<tr>
<td>3DES encryption</td>
<td>Key length of 168 bits</td>
</tr>
<tr>
<td>AES encryption</td>
<td>Key length of 128 or 256</td>
</tr>
</tbody>
</table>

The parameters listed in Table 99 can be modified:

**Table 99  Modifiable policy parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Algorithm</td>
<td>3DES—168-bit key&lt;br&gt;AES-128—128-bit key (default)&lt;br&gt;AES-256—256-bit key</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>SHA-1—Secure Hash Algorithm (default)&lt;br&gt;MD5—Message Digest 5&lt;br&gt;AES-XCBC—Used only for IPSec</td>
</tr>
<tr>
<td>Security Association lifetime in seconds</td>
<td>The lifetime in seconds of the security association. If PFS is enabled, a new IKE SA using new key material will be negotiated before this value expires. Default is 28800 sec.</td>
</tr>
<tr>
<td>PFS (Perfect Forward Secrecy)</td>
<td>Applies only to IKE policies. Choices are On/Off and default is On.</td>
</tr>
<tr>
<td>Diffie-Hellman group</td>
<td>Group 1—768 bits (default)&lt;br&gt;Group 14—2048 bits</td>
</tr>
</tbody>
</table>
Managing policies

Use the `policy` command to create, delete, and show IKE and IPSec policies.

To create a new policy:

1. Log in to the switch as admin.
2. At the command prompt, type:

   ```bash
   policy --create type number [-enc encryption_method] [-auth authentication_algorithm] [-pfs off|on] [-dh DH_group] [-seclife secs]
   ```

   where:

   - `type` and `number` The type of policy being created (IKE or IPSec) and the number for this type of policy. To easily determine how many policies have been created, consider using sequential numbering. The range of valid values is any whole number from 1 through 32.
   - `encryption_method` The supported type of encryption. Valid options are 3DES, AES-128, and AES-256. AES-128 is the default.
   - `authentication_algorithm` The authentication algorithm. Valid options are SHA-1, MD5, and AES-XCBC (IPSec only). SHA-1 is the default.
   - `DH_Group` The Diffie-Hellman group. Supported groups are Group 1 and Group 14. Group 1 is the default.
   - `secs` The security association lifetime in seconds. 28800 is the default.

   The following example shows how to create IKE policy number 10 using 3DES encryption, MD5 authentication, and Diffie-Hellman Group 1:

   ```bash
   switch:admin06> policy --create ike 10 -enc 3des -auth md5 -dh 1
   The following policy has been set:
   ```

   **IKE Policy 10**
   
   Authentication Algorithm: MD5
   Encryption: 3DES
   Perfect Forward Secrecy: on
   Diffie-Hellman Group: 1
   SA Life (seconds): 28800

   Operation Succeeded

   For a complete description of the `policy` command, see the *Fabric OS Command Reference*.

   To display policy settings

   1. To display the settings for a single policy, type:

      ```bash
      policy --show type number
      ```

      For example, to view the IPSec 1 policy, type:

      ```bash
      policy --show ipsec 1
      ```

   2. To display the policy settings for all defined policies, type:

      ```bash
      policy --show type all
      ```
The example below shows all of the IKE policies defined; in this example, there are two IKE policies.

```
switch:admin06> policy --show ike all
IKE Policy 1
-----------------------------------------
Authentication Algorithm: MD5
Encryption: 3DES
Perfect Forward Secrecy: off
Diffie-Hellman Group: 1
SA Life (seconds): 0

IKE Policy 32
-----------------------------------------
Authentication Algorithm: SHA-1
Encryption: AES-128
Perfect Forward Secrecy: on
Diffie-Hellman Group: 1
SA Life (seconds): 28800
```

Policies cannot be modified. You must delete and then recreate a policy with the new parameters.

To delete a policy:

1. Log in to the switch as admin.
2. Enter the following command.

   ```
policy --delete type number
   
   where type is the policy type and number is the number assigned.
   For example, to delete the IPSec policy number 10:
   
   switch:admin06> policy --delete ipsec 10
   The policy has been successfully deleted.
   ```

To view IPSec information for an FCIP tunnel:

The following example shows the `portShow fciptunnel` command used to display IPSec information for tunnel 0:

```
switch:admin06> portshow fciptunnel 8/ge0 3 -ipsec
Port: ge0
-------------------------------------------
Tunnel ID 3
Remote IP Addr 192.175.5.200
Local IP Addr 192.175.5.100
Remote WWN Not Configured
Local WWN 10:00:00:05:1e:37:00:20
Compression off
Fastwrite on
Tape Pipelining on
Uncommitted bandwidth, minimum of 1000 Kbps (0.001000 Gbps)
```

434 Configuring and monitoring FCIP extension services
Persistently disabling ports

Ports used on an FCIP tunnel must be persistently disabled before you can configure FCIP tunnels. You must change their state from persistently disabled to persistently enabled.

1. Enter the `portCfgShow` command to view ports that are persistently disabled.
2. After identifying the ports, enter the `portCfgPersistentDisable` command to disable any ports that you will use in the FCIP tunnel configuration.

Configuring VEX ports

If you are going to use a VEX port in your tunnel configuration, use the `portCfgVexport` command to configure the port as a VEX port. Remember that a VEX port must be paired with a VE port. VEX ports cannot communicate with other VEX ports. The command syntax is as follows.

```
portcfgvexport [slot/]ge0|ge1 [-a 1|2] [-f fabricid] [-d domainid] [-p 1|2|3] [-t 1|2]
```

Where:

- `slot` The number of a slot in a 4/256 SAN Director or DC SAN Backbone Director (short name, DC Director) chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.
- `ge0|ge1` The Ethernet port used by the tunnel (ge0 or ge1).
- `-a 1|2` Enables or disables admin (1 to enable or 2 to disable).
- `-f fabricid` The fabric ID (a number from 1 to 128).
- `-d domainid` The preferred Domain ID (a number from 1 to 239).
- `-p 1|2|3` The port ID format (1 for core, 2 for extended edge, and 3 for native).
- `-t 1|2` Specify 1 to enable or 2 to disable negotiate fabric parameters.
Configuring IP interfaces and IP routes

The IP network connection between two 400 Multi-protocol Router or two FR4-18i blades is configured by defining IP interfaces for origin and destination virtual ports, and then defining one or more IP routes to connect them.

1. Define the IP interface of each virtual port, using the `portcfg` command. You can define up to eight IP interfaces per GbE port. The command syntax is as follows.

   `portcfg ipif [slot/]ge0|ge1 create ipaddr netmask mtu_size`

   Where:
   - `slot` The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.
   - `ge0|ge1` The Ethernet port used by the tunnel (ge0 or ge1).
   - `ipaddr` The IP address of the virtual port.
   - `netmask` The network mask.
   - `mtu_size` The maximum transmission unit size. The range allowed is 1500 to 2284 KB. The default value is 1500 KB, which is the normal value in an Ethernet network. Some networks support jumbo packets (packets larger than 1500 KB). If the network you are using supports jumbo packets, a value of 2284 can improve performance.

   By default, the virtual ports will automatically become VE_Ports.

2. Define IP routes on a GbE port. After defining the IP interface of the remote switch, you can define destination routes on an interface. You can specify a maximum of 32 routes per GbE port. The command syntax is as follows.

   `portcfg iproute [slot/]ge0|ge1 create ipaddr netmask gateway_router metric`

   Where:
   - `slot` The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.
   - `ge0|ge1` The Ethernet port used by the tunnel (ge0 or ge1).
   - `ipaddr` The IP address of the destination virtual port.
   - `netmask` The network mask.
   - `gateway_router` The IP address of an IP router that can route packets to the destination virtual port IP address. The gateway address must be on the same IP subnet as one of the port IP addresses.
   - `metric` A number from 1 to 16 that assigns a cost value to a route. A route that has only one hop has a low cost value, and should be assigned a cost value of 1. Routes with low cost values are chosen first. The metric number is sometimes used to indicate the actual number of hops, but it is used only as a relative value. A low value encourages the use of the route, and a high value discourages the use of a route.

   The following example shows two routes being added to an interface:

   ```
   switch:admin06> portcfg iproute 8/ge0 create 192.168.11.0
   255.255.255.0 192.168.100.1 1
   switch:admin06> portcfg iproute 8/ge0 create 192.168.12.0
   255.255.255.0 192.168.100.1 1
   ```
The following example verifies that the two routes have been successfully created:

```
switch:admin06> portshow iproute 8/ge0
```

```
Slot: 8 Port: ge0
IP Address      Mask            Gateway         Metric  Flags
--------------------------------------------------------------
----
192.168.100.0   255.255.255.0   192.168.100.40   0
Interface
192.168.100.0   255.255.255.0   192.168.100.41   0
Interface
192.168.11.0    255.255.255.0   192.168.100.1    1
192.168.12.0    255.255.255.0   192.168.100.1    1
```

3. If you are implementing VLAN tagging, create a static ARP entry for the IP interfaces on both ends of the tunnel, using the `portcfg arp` command with the `add` option. The command syntax is as follows.

```
portcfg arp [slot/]ge0|ge1 add ipaddr macaddr
```

You can obtain the MAC address (`macaddr`) by using the `portshow arp` command with the `-lmac` option.

4. Verify IP connectivity by entering the `portCmd --ping` command to test the connection to a destination IP address from a source IP address on one of the local Ethernet ports (Ge0 or Ge1). This verification also ensures that data packets can be sent to the remote interface. You can test a connection only if both ports have IP interfaces set. The command syntax is as follows.

```
portcmd --ping [slot/]ge0|ge1 [-s source_ip] [-d dest_ip] [-c L2 class-of-service]
[-n num-requests] [-q type-of-service] [-t ttl] [-v vlan tag] [-w wait-time] [-z size]
```

Where:

- `slot` The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.
- `ge0|ge1` The Ethernet port used by the tunnel (ge0 or ge1).
- `-s source_ip` The source IP interface that originates the ping request.
- `-d destination_ip` The destination IP address for the ping request.
- `-c class-of-service` The Layer 2 class of service (L2CoS).
- `-n num-requests` The number of ping requests to make. The default is 4.
- `-q type-of-service` The DiffServ QoS. The default is 0 (zero). The value must be an integer in the range from 0 through 255.
- `-t ttl` The time to live. The default value is 100.
- `-v vlan tag` The vlan tag for a VLAN tagged IP connection.
- `-w wait-time` The time to wait for the response of each ping request. This parameter is specified in milliseconds and the default value is 5000 milliseconds (5 sec). The maximum allowed wait time for ping is 9000 milliseconds (9 sec).
- `-z size` The size in bytes of the ping packet to use. The total size cannot be greater than the configured MTU size (refer to step 1). The default size is 64 bytes.
The following example tests the connection between 192.175.5.100 and 192.175.5.200,

```
switch:admin06> portcmd --ping ge0 -s 192.175.5.100 -d 192.175.5.200
Pinging 192.175.5.200 from ip interface 192.175.5.100 on 0/ge0 with 64 bytes of data
Reply from 192.175.5.200: bytes=64 rtt=1ms ttl=64
Reply from 192.175.5.200: bytes=64 rtt=0ms ttl=64
Reply from 192.175.5.200: bytes=64 rtt=0ms ttl=64
Reply from 192.175.5.200: bytes=64 rtt=1ms ttl=64
```

Ping Statistics for 192.175.5.200:
   Packets: Sent = 4, Received = 4, Loss = 0 (0 percent loss)
         Min RTT = 0ms, Max RTT = 1ms Average = 0ms

5. Test end-to-end IP path performance using WAN analysis tools (optional, may be done at any time). Refer to “WAN performance analysis tools” on page 451 for specific information and instructions.

**NOTE:** The general recommendation is to run `iperf` only when there are no active tunnels on the IP network. For more information, refer to “About the ipperf option” on page 451.

### Configuring FCIP tunnels

After you have verified licensing and connectivity between source and destination IP interfaces, you can configure FCIP tunnels. As you plan the tunnel configurations, be aware that uncommitted rate tunnels use a minimum of 1000 Kbps, up to a maximum of available uncommitted bandwidth on the GbE port. The total bandwidth available on a GbE port is 1 Gbps. You can configure tunnels as bidirectional entities with different commit rates in both directions.

**NOTE:** You cannot create FCIP tunnels that connect to an HP StorageWorks MP Router.

The command syntax is as follows.

```
portcfg fc iptunnel [slot/]ge0|ge1 create tunnel_id remote_ip_addr
```

Where:

- **slot**
  - The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.
- **ge0/ge1**
  - The Ethernet port used by the tunnel (ge0 or ge1).
- **tunnel_id**
  - The tunnel number (0-7).
- **remote_ip_addr**
  - The IP address for the remote end of the tunnel.
- **local_ip_addr**
  - The IP address for the local end of the tunnel.
- **comm_rate**
  - The committed comm rate for the tunnel.
- **-c**
  - Enables compression on this tunnel.
- **-s**
  - Disables selective acknowledgement code (SACK) on the specified tunnel.
The following example creates one end of a tunnel over ge0 between remote IP address 192.168.10.1 and local IP address 192.168.20.1 with a tunnel id of 0, over VLAN 100, with a layer 2 class of service of 3 for control traffic, and a layer 2 class of service of 7 for data traffic.

```
portcfg fciptunnel 8/ge0 create 192.168.10.1 192.168.20.1 0 -v 100 -p 3 -P 7
```

Configuring FICON emulation

Before you configure FICON emulation, you will need to understand the available options, and if those options are to be implemented in your installation. If FICON emulation is new to you, please read “FICON emulation concepts” on page 428. The syntax for the `portcfg ficon` command is as follows:

```
portcfg ficon [slot/]ge0/ge1 tunnel_Id config [-x 1|0] [-w 1|0] [-r 1|0] [-t 1|0] [-1 1|0] [-b 1|0] [wrtMaxPipe value] [rdMaxPipe value] [wrtMaxDevs value] [rdMaxDevs value] [wrtTimer value] wrtMaxChains value] [oxidBase value] [dbgFlags value]
```
Where:

slot
The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.

g0/e1
The Ethernet port used by the tunnel (ge0 or ge1).
tunnel_id
The tunnel number (0 - 7).
cfg
The config option creates a configuration.
-x 1/0
Enables or disables XRC emulation. 1 is enable, 0 is disable.
-w 1/0
Enables or disables tape write pipelining. 1 is enable, 0 is disable.
-r 1/0
Enables or disables tape read pipelining. 1 is enable, 0 is disable.
-t 1/0
Enables or disables TIN/TIR emulation. 1 is enable, 0 is disable.
-i 1/0
Enables or disables device level ACK emulation. 1 is enable, 0 is disable.
-b 1/0
Enables or disables FICON read block ID. 1 is enable, 0 is disable.

wrtMaxPipe value
Defines a maximum number of channel commands that may be outstanding at a given time during write pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The default value is 32. The range is 1-100.

dmaMaxPipe value
Defines a maximum number of channel commands that may be outstanding at a given time during read pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The default value is 32. The range is 1-100.

wrtMaxDevs value
Defines a maximum number of concurrent emulated tape write operations. The default value is 16. The range is 1-32.

dmaMaxDevs value
Defines a maximum number of concurrent emulated tape read operations. The default value is 16. The range is 1-32.

wrtTimer value
Defines a time limit for pipelined write chains. This value is be specified in milliseconds (ms). If a pipelined write chain takes longer than this value to complete, the ending status for the next write chain will be withheld from the channel. This limits processing to what the network and device can support. Too small a value limits pipelining performance. Too large a value results in too much data being accepted for one device on a path. The default value is 300 milliseconds (ms). The range is 100-1500.

wrtMaxChains value
Defines the maximum amount of data that can be contained in a single CCW chain. If this value is exceeded, emulation is suspended. The default is 3, which represents 3000000 bytes.

oxidBase value
Defines the base value of an entry pool of 256 OXIDs supplied to emulation generated exchanges. It should fall outside the range used by FICON channels and devices to avoid conflicts. The default value is 0x1000. The range is 0x0000 to 0xF000.

dbgFlags value
Defines optional debug flags. The default is 0xF7C80000. This is primarily for use by technical support personnel.

The following example shows FICON emulation on ge0 over tunnel id 1 with FICON XRC and tape write pipelining enabled. The default values are assumed for wrtMaxPipe, wrtMaxDev, wrtTimer, and wrtMaxChains.

portcfg ficon ge0 config -x 1 -w 1
Configuring FTRACE

FTRACE is a support tool primarily for use by Tech Support personnel. FTRACE includes the ability to freeze traces on certain events, and to retain the trace information for future examination. The syntax for the `portcfg ftrace` command is as follows:

```bash
portcfg ftrace [slot/][ge0|ge1] tunnel_Id cfg [-a 1|0] [-b value] [-e 1|0] [-i value] [-p value] [-r value] [-s value] [-t value] [-z value]
```

Where:

- **slot**: The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.
- **ge0|ge1**: The Ethernet port used by the tunnel (ge0 or Ge1).
- **tunnel_Id**: The tunnel number (0 - 7).
- **cfg**: Creates an FTRACE configuration.
- **-a 1|0**: Enables or disables ACO.
- **-b value**: Number of buffers (range 0 to 8).
- **-e 1|0**: Enable or disable FTRACE.
- **-i value**: Display mask value (range 0 to FFFFFFFF).
  Default is FFFFFFFF.
- **-p value**: Post trigger percentage value (range 0-100). Default is 5.
- **-r value**: Number of records (range 0 through 1,677,721). Default us 200000.
- **-s value**: Trigger mask value (range 00000000 to FFFFFFFF). Default us 000000003.
- **-t value**: Trace mask value (range 00000000 to FFFFFFFF). Default is 80000C7B.
- **-z value**: Trace record size (range 80 to 240). Default is 80.

The following example configures FTRACE with ACO disabled, and FTRACE enabled with a trigger mask value of 00000003, and a trace mask value of ffffffff.

```bash
portcfg ftrace ge0 3 cfg -a 0 -e 1 -p 5 -s 00000003 -t ffffffff
```

Verifying the FCIP tunnel configuration

After you have created local and remote FCIP configurations, it is recommended that you verify that the tunnel configuration operation succeeded using the `portShow fcipTunnel` command (be sure to specify the slot/port numbers and number of tunnels). The command syntax is as follows:

```bash
portshow fcipTunnel [slot/] [ge0|ge1 all|tunnel_id]
```

Where:

- **all**: Displays all FCIP tunnels.
- **tunnel_id**: Displays the specified FCIP tunnel.
The following example shows an active tunnel with FCIP fastwrite and tape pipelining enabled:

```
switch:admin06> portshow fciptunnel ge0 all
-------------------------------------------
Tunnel ID 0
Remote IP Addr 10.0.10.224
Local IP Addr 10.0.10.225
Remote WWN Not Configured
Local WWN 10:00:00:05:1e:37:91:dd
Compression on
Fastwrite on
Tape Pipelining on
Uncommitted bandwidth, minimum of 1000 Kbps (0.001000 Gbps)
SACK on
Min Retransmit Time 100
Keepalive Timeout 10
Max Retransmissions 8
DSCP Marking (Control): 10, DSCP marking (Data): 50
Status : Active
Uptime 21 seconds

IKE Policy 1
Authentication Algorithm: SHA-1
Encryption: 3DES
Perfect Forward Security: off
Diffie-Hellman Group: 1
SA Life (seconds): 3600
SA Life (MB): 4500
IPSec Policy 1
Authentication Algorithm: SHA-1
Encryption: 3DES
Perfect Forward Security: off
Diffie-Hellman Group: 1
SA Life (seconds): 3600
SA Life (MB): 4500
Pre-Shared Key 0x1234500000000000000000000000000000000000
```

If IPSec has been enabled and a policy added to the configuration, you will see the policy information under the status section of the output, as shown below. The policy information is visible only when IPSec is configured and is displayed with the information shown in the example above when the `portShow` command is issued.

```
IKE Policy 1
Authentication Algorithm: SHA-1
Encryption: 3DES
Perfect Forward Security: off
Diffie-Hellman Group: 1
SA Life (seconds): 3600
SA Life (MB): 4500
IPSec Policy 1
Authentication Algorithm: SHA-1
Encryption: 3DES
Perfect Forward Security: off
Diffie-Hellman Group: 1
SA Life (seconds): 3600
SA Life (MB): 4500
Pre-Shared Key 0x1234500000000000000000000000000000000000
```

After FCIP tunnels are created, the configuration is saved in a persistent database. At this point, all configured FCIP tunnels now appear in the fabric as VE_Ports.
To verify that a VE_Port or VEX_Port is online, use the `switchShow` command to view and verify that the FCIP tunnel is online.

```
switch:admin06> portenable 8/18
switch:admin06> portenable 8/19
switch:admin06> switchshow

switchName: switch
switchType: 42.2
switchState: Online
switchMode: Native
switchRole: Subordinate
switchDomain: 4
switchId: ffff04
switchWwn: 10:00:00:60:69:80:0d:bc
zoning: ON (LSAN001)
switchBeacon: OFF
blade3 Beacon: OFF
blade4 Beacon: OFF
blade8 Beacon: OFF
FC router: ON
FC router BB Fabric ID: 1

<table>
<thead>
<tr>
<th>Area</th>
<th>Slot</th>
<th>Port</th>
<th>Media</th>
<th>Speed</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>3</td>
<td>0</td>
<td>id</td>
<td>N4</td>
<td>Online F-Port</td>
</tr>
<tr>
<td>33</td>
<td>3</td>
<td>1</td>
<td>id</td>
<td>N4</td>
<td>Online F-Port</td>
</tr>
<tr>
<td>34</td>
<td>3</td>
<td>2</td>
<td>id</td>
<td>N4</td>
<td>Online F-Port</td>
</tr>
<tr>
<td>35</td>
<td>3</td>
<td>3</td>
<td>id</td>
<td>N4</td>
<td>Online F-Port</td>
</tr>
<tr>
<td>36</td>
<td>3</td>
<td>4</td>
<td>id</td>
<td>N2</td>
<td>Online F-Port</td>
</tr>
</tbody>
</table>
```

210 8 18 -- -- Online VE-Port
211 8 19 -- -- Online VE-Port

223 8 31 -- -- Offline

8 ge0 id 1G Online
8 ge1 id 1G Online
Enabling persistently disabled ports

Before an FCIP tunnel can be used, the associated ports must be persistently enabled.

**NOTE:** VEX_Port Users: If the fabric is already connected, you must leave the ge0 and ge1 ports disabled until after you have configured the VEX Port; this will prevent unintentional merging of the two fabrics.

To enable a persistently disabled port:

1. Enter the `portCfgShow` command to view ports that are persistently disabled.
2. After identifying the ports, enter the `portCfgPersistentEnable` command to enable the ports.
3. Enter the portCfgShow command to verify the port is persistently enabled as shown below:

```
switch:admin06> portcfgpersistentenable 8/16
switch:admin06> portcfgpersistentenable 8/17
switch:admin06> portcfgpersistentenable 8/18
switch:admin06> portcfgpersistentenable 8/19

switch:admin06> portcfgshow
Ports of Slot 8    0  1  2  3    4  5  6  7    8  9 10 11   12 13 14 15
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+
              --
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
RSCN Suppressed   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent DisableON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
EX Port           .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Mirror Port       .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..

Ports of Slot 8   16 17 18 19   20 21 22 23   24 25 26 27   28 29 30 31
-----------------+--+--+--+--+----+--+--+--+----+--+--+--+----+--+--+
              --
Speed             AN AN AN AN   AN AN AN AN   AN AN AN AN   AN AN AN AN
Trunk Port        ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
Long Distance     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
VC Link Init      .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked L_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Locked G_Port     .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Disabled E_Port   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
ISL R_RDY Mode    .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
RSCN Suppressed   .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Persistent Disable.. .. ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
NPIV capability   ON ON ON ON   ON ON ON ON   ON ON ON ON   ON ON ON ON
EX Port           .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..
Mirror Port       .. .. .. ..   .. .. .. ..   .. .. .. ..   .. .. .. ..

where AN:AutoNegotiate, ..:OFF, ??:INVALID.

LM:L0.5
```

switch:admin06>
Modify and delete command options

Command options are available that allow you to modify or delete configured elements.

**NOTE:** Using the *Modify* option disrupts traffic on the specified FCIP tunnel for a brief period of time.

Modifying FCIP tunnels

The `portCfg fcipTunnel` command to modify FCIP tunnels (you must specify at least one characteristic to modify). The command syntax is as follows:

```
portcfg fcipTunnel [slot/]
port modify tunnel_id [-b comm_rate] [-c 0|1]
[-s 0|1] [-f 0|1] [-k timeout] [-m time] [-q control_dscp] [-Q data_dscp] [-P control_L2Cos]
[-p data_L2Cos] [-r retransmissions] [-t 0|1]
```

Where:

- **slot**: The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.
- **port**: The Ethernet port used by the tunnel (ge0 or Ge1).
- **tunnel_id**: The tunnel number (0 - 7).
- **modify**: The modify option changes the FCIP tunnel configuration options and parameters.
- **-b comm_rate**: New committed traffic rate in Kb/sec on the existing FCIP tunnel.
- **-c 0|1**: Disables (0)/Enables (1) compression on the existing FCIP tunnel.
- **-s 0|1**: SACK ON (1)/SACK OFF (0) on the existing FCIP tunnel.
- **-f 0|1**: Enables (1)/Disables (0) FCIP fastwrite.
- **-M 0|1**: Enables or disables VC QoS mapping.
- **-t 0|1**: Enables (1)/Disables (0) tape pipelining on the existing tunnel. If tape pipelining is enabled, you must also enable fastwrite.
- **-k timeout**: The new keep-alive timeout on the existing FCIP tunnel. A range of valid values is 8 through 7200 sec. If tape pipelining is enabled, the default and minimum value is 80 sec.
- **-m time**: The new minimum retransmit time for the existing FCIP tunnel. A range of valid values is 20 through 5000 ms (milliseconds).
- **-r retransmissions**: The maximum number of retransmissions on the existing FCIP tunnel. A range of valid values is 1 through 16. If tape pipelining is enabled, the number of retransmissions is calculated based on the minimum retransmit time to ensure that the tunnel does not time out before the host times out (about 80 sec). If you change this value, the value specified must be greater than the calculated value.
- **-q control_dscp**: The DSCP marking for the FCIP tunnel’s TCP control connection. The range of valid values is 0 through 63. The default is 0. Before configuring DSCP settings, determine if the IP network you are using implements PHB, and consult with the network administrator to determine the appropriate DSCP values.
- **-Q data_dscp**: The DSCP marking for the FCIP tunnel’s TCP data connection. The range of valid values is 0 through 63. The default is 0. Before configuring DSCP settings, determine if the IP network you are using implements PHB, and consult with the network administrator to determine the appropriate DSCP values.
The following example shows two FCIP tunnels created on slot 8, port ge0; the first with an uncommitted bandwidth (0), and the second with a committed bandwidth of 10000 Kb/sec:

```
switch:admin06> portcfg fciptunnel 8/ge0 create 2 192.168.100.50
192.168.100.40 0
switch:admin06> portcfg fciptunnel 8/ge0 create 3 192.168.100.51
192.168.100.41 10000
```

The following example shows an FCIP tunnel created between a remote interface <10.1.1.44>, and a local IP interface <192.168.131.124>:

```
switch:admin06> portcfg fciptunnel 3/ge0 create 6 10.1.1.44
192.168.131.124 155000
```

### Modifying/deleting QoS Settings

The QosMap option of the `portCfg fciptunnel` command allows you to modify QoS settings or delete the QosMap configuration file for a virtual port. The command syntax is as follows:

```
portCfg fciptunnel [Slot/]ge0|ge1 qosmap tunnel_id virtual_channel -default
-delete -Q data-dscp -P data-L2cos
```

Where:

- **-default** resets the VC QoS map to default values.
- **-delete** deletes the associated QoS map configuration file. The -delete option is used before firmware downgrades to versions previous to Version 6.0.0 that do not support QoS mapping. It removes the file from the config flash memory only. The file is automatically created to defaults if later used or modified.
- **-Q data-dscp** modifies the Diffserv marking value.
- **-P data-L2cos** modifies the L2 Class of Service tagging value.

**NOTE:** Modified values are not reset to defaults when the tunnel QoS is disabled and enabled. If you want to revert to default values, use the `-default` option.

### FICON emulation modify operations

Following is the syntax for the `portcfg ficon modify` command:

```
portcfg ficon [slot/]ge0|ge1 tunnel_Id modify [-x 1|0] [-w 1|0] [-r 1|0] [-t 1|0] [-l 1|0] [-b 1|0] [wrtMaxPipe value] [rdMaxPipe value] [wrtMaxDevs value] [rdMaxDevs value] [wrtTimer value] [wrtMaxChains value] [oxidBase value] [dbgFlags value] [xrcErr] [LrcCheck]
```

Where:

- **slot** The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.
- **ge0|ge1** The Ethernet port used by the tunnel (ge0 or Ge1).
- **tunnel_id** The tunnel number (0 - 7).
The modify option changes the FICON emulation configuration options and parameters.

The following options turn features on and off. The associates tunnels must be disabled to modify the option settings. If you attempt to do them on an enabled tunnel, the operation is not allowed, and you are prompted to disable the tunnel.

- \(-x\) \(1|0\) Enables or disables XRC emulation. 1 is enable, 0 is disable.
- \(-w\) \(1|0\) Enables or disables tape write pipelining. 1 is enable, 0 is disable.
- \(-r\) \(1|0\) Enables or disables tape read pipelining. 1 is enable, 0 is disable.
- \(-t\) \(1|0\) Enables or disables TIN/TUR emulation. 1 is enable, 0 is disable.
- \(-l\) \(1|0\) Enables or disables device level ACK emulation. 1 is enable, 0 is disable.
- \(-b\) \(1|0\) Enables or disables FICON read block ID. 1 is enable, 0 is disable.

The following parameters may be modified on active tunnels.

- **wrtMaxPipe value**
  Defines a maximum number of channel commands that may be outstanding at a given time during write pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The default value is 32. The range is 1-100.

- **rdMaxPipe value**
  Defines a maximum number of channel commands that may be outstanding at a given time during read pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The default value is 32. The range is 1-100.

- **wrtMaxDevs value**
  Defines a maximum number of concurrent emulated tape write operations. The default value is 16. The range is 1-32.

- **rdMaxDevs value**
  Defines a maximum number of concurrent emulated tape read operations. The default value is 16. The range is 1-32.

- **wrtTimer value**
  Defines a time limit for pipelined write chains. This value is specified in milliseconds (ms). If a pipelined write chain takes longer than this value to complete, the ending status for the next write chain will be withheld from the channel. This limits processing to what the network and device can support. Too small a value limits pipelining performance. Too large a value results in too much data being accepted for one device on a path. The default value is 300 milliseconds (ms). The range is 100-1500.
Deleting an fcip tunnel

Following is the syntax for the `portCfg fcipTunnel` command to delete FICP tunnels:

```
portcfg fciptunnel [slot/]ge0|ge1 delete tunnel_id
```

The following example shows two tunnels deleted on slot 8, port ge0:

```
switch:admin06> portcfg fciptunnel 8/ge0 delete 6
switch:admin06> portcfg fciptunnel 8/ge0 delete 7
```

Deleting an IP interface (IPIF)

The following command deletes an IP interface.

```
portcfg ipif delete ipaddr
```

Deleting an IRoute

The following command deletes an IP route.

```
portcfg iproute [slot/]ge0|ge1 delete ipaddr netmask
```

Deleting an FTRACE configuration

The following command deletes an FTRACE configuration.

```
portcfg ftrace ge0 3 del
```

Maintaining VLAN tag tables

The VLAN tag table is used by ingress processing to filter inbound VLAN tagged frames. If a VLAN tagged frame is received from the network and there is no entry in the VLAN tag table for the VLAN ID, the frame is discarded.

The table is used to determine how to tag a frame that is not already tagged. To tag frames destined for a specific host address, you must create an entry with an exact matching destination address in the table. Only frames destined for that address are tagged with the associated VLAN ID. To tag frames destined for a specific network, you must create a destination address entry for the network. For example, if a destination address of 192.168.100.0 is specified, then all frames destined for the 192.168.100.0 network are tagged with the associated VLAN ID, assuming a network mask of 255.255.255.0. If an entry contains a destination address of 0.0.0.0, all frames are tagged with the associated VLAN ID. If frames are already VLAN tagged, those tags take precedence over entries in this table.
NOTE: If you do not specify a destination IP address, the destination address defaults to 0.0.0.0, and all frames are tagged with the associated VLAN tag.

FCIP and ipPerf create and maintain entries in the VLAN tag table through their own configuration procedures. Manual entries are needed on both the local and remote sides for portcmd ping and portcmd traceroute commands when they are used to test and trace routes across a VLAN when no FCIP tunnel is active.

The following The portCfg vlantag command is used to add or delete entries in the VLAN tag table. The syntax for the portCfg vlantag command is as follows:

```
portcfg vlantag add|delete ipif_addr vlan_id L2CoS dest_IP_addr
```

Where:

- `pif_addr` The locally defined IP address.
- `vlan_id` The VLAN tag used for this tag (range 1-4094).
- `L2CoS` Layer 2 class of service (range 0-7)
- `dest_IP_addr` The destination IP address. All frames destined for this IP address will be tagged with the specified vlan_id and L2 CoS. If a destination IP address is not specified, all frames not already tagged will be tagged.

The following example adds an entry that tags all frames from IP address 192.168.10.1 destined for IP address 192.168.20.1 with a VLAN ID of 100, and a L2 CoS value of 3.

```
portcfg vlantag 8/ge0 add 192.168.10.1 100 3 7 192.168.20.1
```

Troubleshooting FCIP links

The following list contains information for troubleshooting FCIP links:

- When deleting FCIP links, you must delete them in the exact reverse order they were created. That is, delete first the tunnels, then the IP interfaces, and finally the port configuration. The IP route information is removed automatically at this point.
- IP addresses are retained by slot in the system. If FR4-18i blades are moved to different slots without first deleting configurations, errors can be seen when trying to reuse these IP addresses.
- The portCmd ping command only verifies physical connectivity. This command does not verify that you have configured the ports correctly for FCIP tunnels.
- One port can be included in multiple tunnels, but each tunnel must have at least one port that is unique to that tunnel.
- Ports at both ends of the tunnel must be configured correctly for an FCIP tunnel to work correctly. These ports can be either VE_Ports or VEX_Ports. A VEX_Port must be connected to a VE_Port.
- When configuring routing over an FCIP link for a fabric, the edge fabric will use VE_Ports and the backbone fabric will use VEX_Ports for a single tunnel.
- If an FCIP tunnel fails with the “Disabled (Fabric ID Oversubscribed)” message, the solution is to reconfigure the VEX_Port to the same Fabric ID as all of the other ports connecting to the edge fabric.
- Due to an IPSec RASLog limitation, you may not be able to determine an incorrect configuration that causes an IPSec tunnel to not become active. This misconfiguration can occur on either end of the tunnel. As a result, you must correctly match the encryption method, authentication algorithm, and other configurations on each end of the tunnel.
WAN performance analysis tools

Introduced in Fabric OS 5.2.0, WAN analysis tools are designed to test connections, trace routes, and estimate the end-to-end IP path performance characteristics between a pair of HP FCIP port endpoints. WAN tools include the following commands and options:

- **portCmd ipPerf**—Charactizes end-to-end IP path performance between a pair of HP FCIP ports. You can use the WAN tool ipPerf only on the FR4-18i or 400 Multi-protocol Router FCIP ports running Fabric OS 5.2.0 or later software.
- **portCmd ping**—Tests connections between a local Ethernet port (ge0 or ge1) and a destination IP address.
- **portCmd traceroute**—Traces routes from a local Ethernet port (ge0 or ge1) to a destination IP address.
- **portShow fcipTunnel**—Displays performance statistics generated from the WAN analysis.

About the ipperf option

The WAN tool ipPerf (referred to simply as "ipPerf" in this chapter) is an option of the Fabric OS portCmd command. This option allows you to specify the slot and port information for displaying performance statistics for a pair of ports. For this basic configuration, you can specify the IP addresses of the endpoints, target bandwidth for the path, and optional parameters such as the length of time to run the test and statistic polling interval.

Only a single ipPerf session can be active on an FCIP GbE port at any time. Each FCIP port supports a single instance of the WAN tool-embedded client running in only sender or receiver mode. You can, however, use multiple CLI sessions to invoke simultaneous ipPerf sessions on different FCIP ports.

Running WAN tool sessions with an FCIP tunnel online

ipPerf sessions use different TCP ports than FCIP tunnels, so you can simultaneously run an ipPerf session between a pair of ports while an FCIP tunnel is online. You can, for example, revalidate the service provider Service Level Agreement (SLA) without bringing the FCIP tunnel down, but the general recommendation is to run ipperf only when there are no active tunnels on the IP network. Data transferred across an active FCIP tunnel competes for the same network bandwidth as the ipPerf session, and ipPerf is attempting to saturate a network to determine how much usable bandwidth is available between the sites. Unless you have a method to quiesce all storage traffic over an active FCIP tunnel during ipPerf testing, you may experience undesirable interactions.

FCIP port bandwidth

Allocation of the FCIP GbE port bandwidth behaves exactly the same for ipPerf as for FCIP tunnels. If bandwidth is allocated for FCIP tunnels, the ipPerf session uses the remaining bandwidth. Since bandwidth is already reserved for the FCIP tunnels, the ipPerf session is not affected by any active FCIP tunnel. If no bandwidth is reserved, the ipPerf session competes for a share of the uncommitted bandwidth. Starting an ipPerf session has an impact on any active uncommitted bandwidth FCIP tunnels just like adding a new FCIP tunnel would. For example:

- Adding a committed-rate ipPerf session reduces the total uncommitted bandwidth shared by all the uncommitted bandwidth FCIP tunnels.
- Adding an uncommitted-bandwidth ipPerf session adds another flow competing for the shared uncommitted bandwidth.

The CLI and configuration system ensures that any bandwidth allocation does not result in an over commitment of the FCIP GbE port. An active FCIP tunnel cannot be forced to give up its committed buffer and bandwidth resources. Therefore, to commit a specific bandwidth to the ipPerf session, you must have an equivalent amount of spare capacity on the FCIP GbE port.
WAN tool performance characteristics

Table 100 lists the end-to-end IP path performance characteristics that you can display using the `portCmd ipPerf` command and option. All four of the base `ipPerf` performance characteristics (bandwidth, loss, RTT, PMTU) are provided in the command output in Fabric OS 5.2.0 or later.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Indicates the total packets and bytes sent. Bytes/second estimates are maintained as a weighted average with a 30 second sampling frequency and also as an average rate over the entire test run. The CLI output prints the bandwidth observed in the last display interval as well as the Weighted Bandwidth (WBW). BW represents what the FCIP tunnel / FC application sees for throughput rather than the Ethernet on-the-wire bytes.</td>
</tr>
<tr>
<td>Loss</td>
<td>Indicates the loss estimate is based on the number of TCP retransmits (assumption is that the number of spurious retransmits is minimal). Loss rate (percentage) is calculated based on the rate of retransmissions within the last display interval.</td>
</tr>
<tr>
<td>Delay</td>
<td>Indicates TCP smoothed RTT and variance estimate in milliseconds.</td>
</tr>
</tbody>
</table>
| Path MTU (PMTU) | Indicates the largest IP-layer datagram that can be transmitted over the end-to-end path without fragmentation. This value is measured in bytes and includes the IP header and payload.  
There is a limited support for black hole PMTU discovery. If the Jumbo PMTU (anything over 1500) does not work, ipPerf will try 1500 bytes (minimum PMTU supported for FCIP tunnels). If 1500 PMTU fails, ipPerf will give up. There is no support for aging. PMTU detection is not supported for active tunnels. During black hole PMTU discovery, the BW, Loss, and PMTU values printed may not be accurate. |

Starting WAN tool analysis

Typically, you start the WAN tool before setting up a new FCIP tunnel between two sites. You can configure and use the `ipPerf` option immediately after installing the IP configuration on the FCIP port (for example, IP address, route entries). Once the basic IP addressing and IP connectivity is established between two sites, you can configure `ipPerf` with parameters similar to what will be used when the FCIP tunnel is configured.

The traffic stream generated by the WAN tool `ipPerf` session can be used for the following functions:

- Validate a service provider Service Level Agreement (SLA) throughput, loss, and delay characteristics.
- Validate end-to-end PMTU, especially if you are trying to eliminate TCP segmentation of large Fibre Channel (FC) frames.
- Study the effects and impact FCIP tunnel traffic may have on any other applications sharing network resources.

To start an `ipPerf` session, you can use any port as long as the port (in combination with local interface) is not in use. You must run the `ipPerf` client on both the host (source mode, `-S` option) and receiver (sink mode, `-R` option). See “WAN tool ipPerf syntax” on page 453 for more information about specifying source and sink mode.
To start an ipPerf session:

1. Configure the receiver test endpoint using the CP CLI.
The syntax for invoking the receiver test endpoint using ipPerf for slot8, port ge0 on an FR4-18i is as follows:

   `portcmd --ipperf 8/ge0 -s 192.168.255.10 -d 192.168.255.100 -R`

2. Configure the sender test endpoint using a similar CP CLI.
The syntax for invoking the sender test endpoint using ipPerf for slot8, port ge0 on an FR4-18i is as follows:

   `portcmd --ipperf 8/ge0 -s 192.168.255.100 -d 192.168.255.10 -S`

The following example shows the results of the performance analysis for slot 8, port ge0:

```
iperf to 192.168.255.10 from IP interface 192.168.255.100 on 8/0:3227
30s: BW:113.03MBps WBW(30s): 55.39MBps Loss(%):0.0 Delay(ms):1 PMTU:1500
60s: BW:108.89MBps WBW(30s): 83.08MBps Loss(%):0.0 Delay(ms):0 PMTU:1500
90s: BW:112.59MBps WBW(30s): 96.93MBps Loss(%):0.0 Delay(ms):0 PMTU:1500
120s: BW:108.93MBps WBW(30s): 103.85MBps Loss(%):0.0 Delay(ms):0 PMTU:1500
150s: BW:112.36MBps WBW(30s): 107.32MBps Loss(%):0.0 Delay(ms):0 PMTU:1500
```

In the example above, **BW** represents Bandwidth and **Delay** represents the round-trip-time (RTT) in milliseconds. The output is printed after each display interval (if you do not specify an interval, the default is 30 seconds). In the output, data is displayed as follows:

- First column—Time elapsed since the start of the test.
- Second column—Bandwidth observed in the last display interval using the following units:
  - MBps—megabytes per second.
  - Mbps—megabits per second
  - KBps—kilobytes per second
  - Kbps—kilobits per second
  - Bps—bytes per second
  - bps—bits per second
- Third column—The 30s weighted bandwidth

**WAN tool ipPerf syntax**

When using the `portCmd ipPerf` option, you must specify the following:

- **Source IP address.** If the `ipPerf` is started with `-S` (source mode), the port number specified is the remote peer’s port number to connect to.
- **Destination IP address.**
- **Source (transmitter) or sink (receiver).** If the `ipPerf` is started with `-R` (sink mode), the port number and source IP address will be used to listen for new connections.

If the options are not specified the following defaults apply:

- **Default port** —3227
- **Default runtime**—forever
- **Default display (refresh) interval**—30 seconds
• Default size—1MSS

Following is the syntax for `portCmd ipPerf` to display end-to-end IP path performance statistics:

```
portCmd --ipPerf [slot]/ge0|ge1 -s source_ip -d destination_ip -S|-R [-r rate] [-z size] [-t time] 
[-i interval] [-p port] [-q diffserv] [-v vlan_id] [-c L2_Cos]
```

Where:

- `-s source_ip` The source IP address.
- `-d destination_ip` The destination IP address.
- `-S` Operates the WAN tool FCIP port-embedded client in the sender mode. The test endpoint will generate a traffic stream and report the end-to-end IP path characteristics from this endpoint toward the receiver endpoint. This option cannot be used with the `-R` option.
- `-R` Operates the WAN tool FCIP-port embedded client in the receiver mode. The test endpoint will accept a connection and traffic stream from the sender. This option cannot be used with the `-S` option.
- `-r rate` The committed rate for the data stream in Kb/s. If specified, the traffic generator will be limited by a traffic shaper. This can be used to characterize the end-to-end IP path performance based on the data rate to be configured for a tunnel between the same endpoints. If a rate is not specified then the traffic generator will compete for uncommitted bandwidth.
- `-z size` The size in bytes for each buffer handed to the TCP layer. If a size is not specified, the maximum size data buffer will be used based on the outbound IP interface MTU. The size is the only buffer size that will be handed over to the TCP layer.
- `-t time` The total time in seconds to run the test traffic stream. If a time is not specified, the test will run continuously until stopped by typing `Ctrl-C`.
- `-i interval` The interval in seconds between polling and printing stats. The default is 30 sec. If this time is greater than the running time (specified by `-I`), the stats will be printed only once at the conclusion of the test.
- `-p port` The TCP port number for the listener endpoint. If a TCP port is not specified, port 3227 is used (this is next port after ports 3225 and 3226, which are used for the FCIP tunnel connections).
- `-q diffserv` The DiffServ marking code point (DSCP) for the TCP connection. The value must be an integer in the range of 0 to 63. The default value is 0. This operand is optional. Before configuring DSCP settings, determine if the IP network you are using implements PHB, and consult with the network administrator to determine the appropriate DSCP values.
- `-v vlan_id` The VLAN ID.
- `-c L2_Cos` The Layer 2 class of service.

Using `portCmd ping`:

The `portCmd ping` command tests the connection between the IP address of a local Ethernet port (ge0 or ge1) and a destination IP address. If you want to use this command to test a VLAN connection when you do not have an active FCIP tunnel, you must manually add entries to the VLAN tag table on both the local and remote sides of the route, using `portCfg vlantag` command.

```
portCmd --ping [slot]/ge0|ge1 -s source_ip -d destination_ip -n num_requests] [-q diffserv] [-t ttl] [-w wait_time] [-z size] [-v vlan_id] [-c L2_Cos]
```
Where:

- **slot**: The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.

- **ge0|ge1**: The Ethernet port used by the tunnel (ge0 or ge1)

- **-s source_ip**: The source IP interface that originates the ping request.

- **-d destination_ip**: The destination IP address for the ping request.

- **-n num-requests**: Generates a specified number of ping requests. The default is 4.

- **-q diffserv**: The DiffServ QoS. The default is 0 (zero). The value must be an integer in the range from 0 through 255.

- **-t ttl**: The time to live (TTL) for the ping packets. The ttl is decremented every time a router handles the packet. If TTL reaches zero, the packet is discarded. This prevents ping packets from circulating forever and potentially flooding the network. The default value is 100.

- **-v vlan tag**: The vlan tag for a VLAN tagged IP connection.

- **-w wait-time**: The time to wait for the response of each ping request. This parameter is specified in milliseconds and the default value is 5000 milliseconds (5 sec). The maximum allowed wait time for ping is 9000 milliseconds (9 sec).

- **-z size**: The size in bytes of the ping packet to use. The total size cannot be greater than the configured MTU size. You can use the portshow ipif command to display the MTU size for ge0 or ge1. The default size is 64 bytes.

- **-v vlan_id**: The vlan tag for a VLAN tagged IP connection.

- **-c L2_Cos**: The Layer 2 class of service (L2CoS).

The following example tests the connection between IP addresses 192.168.10.1 and 192.168.20.1 over VLAN 10 with a layer 2 class of service of 3.

```
portcmd --ping 8/ge0 -s 192.168.10.1 -d 192.168.20.1 -v 10 -c 3
```

**Using portCmd traceroute**

The portCmd traceroute command traces routes from a local Ethernet port (ge0 or ge1) to a destination IP address. If you want to use this command to trace a route across a VLAN when you do not have an active FCIP tunnel, you must manually add entries to the VLAN tag table on both the local and remote sides of the route, using `portCfg vlantag` command.

```
portCmd --traceroute [slot]/ge0|ge1 -s source_ip -d destination_ip [-h max_hops] [-f first_ttl] [-q diffserv] [-w timeout] [-z size] [-v vlan_id] [-c L2_Cos]
```

Where:

- **slot**: The number of a slot in a 4/256 SAN Director or DC Director chassis that contains an FR4-18i blade. This parameter does not apply to the stand-alone 400 Multi-protocol Router.

- **ge0|ge1**: The Ethernet port used by the tunnel (ge0 or ge1)

- **-s source_ip**: The source IP interface that originates the traceroute request.

- **-d destination_ip**: The destination IP address for the traceroute request.
The following example traces the route between IP addresses 192.168.10.1 and 192.168.20.1 over VLAN 10.

```
portcmd --traceroute 8/ge0 -s 192.168.10.1 -d 192.168.20.1 -v 10
```

**FCIP tunnel performance characteristics**

You can use the `portShow fcipTunnel` command to view the performance statistics and monitor the behavior of an online FCIP tunnel. To view detailed fcipTunnel statistics, you must specify either the `-perf` or `-params` options. The command syntax is as follows.

```
switch:admin06> portshow fcipTunnel [Slot]/ge0|ge1 -perf -params
```

The following example shows the `portCmd fcipTunnel with the -perf option to display performance characteristics of tunnel 0.

```
switch:admin06> portshow fcipTunnel 8/ge0 all -perf
Slot: 8 Port: ge0

-------------------------------------------
Tunnel ID 0
Remote IP Addr 192.175.4.200
Local IP Addr 192.175.4.100
Remote WWN Not Configured
Local WWN 10:00:00:60:69:e2:09:be
Compression on
Fastwrite off
Committed Rate 300000 Kbps (0.300000 Gbps)
SACK on
Min Retransmit Time 100
Keepalive Timeout 10
Max Retransmissions 8
Status: Active
Uptime 7 minutes, 3 seconds
QoS shaper performance stats:
14808626616 Bytes
39615391 Bps 30s avg, 35006573 Bps lifetime avg
```
2013762456 compressed Bytes
33208083 Bps 30s avg, 4760667 Bps lifetime avg
7.35 compression ratio

FC control traffic TCP connection:
Local 192.175.4.100:4139, Remote 192.175.4.200:3225

Performance stats:
849 output packets
0 pkt/s 30s avg, 2 pkt/s lifetime avg
173404 output Bytes
39 Bps 30s avg, 409 Bps lifetime avg
0 packets lost (retransmits)
0.00% loss rate 30s avg
806 input packets
0 pkt/s 30s avg, 1 pkt/s lifetime avg
116736 input Bytes
35 Bps 30s avg, 275 Bps lifetime avg

Data transfer TCP connection:
Local 192.175.4.100:4140, Remote 192.175.4.200:3226

Performance stats:
12899612 output packets
34508 pkt/s 30s avg, 30495 pkt/s lifetime avg
14499127648 output Bytes
38787792 Bps 30s avg, 34276897 Bps lifetime avg
0 packets lost (retransmits)
0.00% loss rate 30s avg
6495624 input packets
17381 pkt/s 30s avg, 15356 pkt/s lifetime avg
207859776 input Bytes
556200 Bps 30s avg, 491394 Bps lifetime avg

The following example shows the portCmd fcipTunnel with the parameters options to display the parameters of tunnel 0:

switch:admin06> portshow fciptunnel 8/ge0 0 –params
Slot: 8 Port: ge0
-------------------------------------------
Tunnel ID 0
Remote IP Addr 192.175.4.200
Local IP Addr 192.175.4.100
Remote WWN Not Configured
Local WWN 10:00:00:60:69:e2:09:be
Compression on
Fastwrite off
Committed Rate 300000 Kbps (0.300000 Gbps)
SACK on
Min Retransmit Time 100
Keepalive Timeout 10
Max Retransmissions 8
Status : Active
Uptime 7 minutes, 3 seconds
FC control traffic TCP connection:
  Local 192.175.4.100:4139, Remote 192.175.4.200:3225
Runtime parameters:
  Send MSS 1456 Bytes
Sender stats:
  smoothed roundtrip 50 ms, variance 0
  peer advertised window 1874944 Bytes
  negotiated window scale (shift count) 9
  congestion window 149649 Bytes
  slow start threshold 1875000 Bytes
  operational mode: slow start
  2 packets queued: TCP sequence# MIN(2950582519)
                      MAX(2950582655) NXT(2950582655)
  2 packets in-flight
  Send.Unacknowledged(TCP sequence# 2950582519) recovery:
    retransmit timeout 500 ms, duplicate ACKs 0
  retransmits 0 (max retransmits 8)
  loss recovery: fast retransmits 0, retransmit timeouts 0
Receiver stats:
  advertised window 1874944 Bytes (max 1874944)
  negotiated window scale (shift count) 9
  0 packets queued: TCP sequence# NXT(2101820798)
  0 out-of-order packets queued (0 lifetime total)
Keepalive:
  time since last activity detected 0 s
  idle connection probe interval 1 s
  timeout 10 s
Data transfer TCP connection:
  Local 192.175.4.100:4140, Remote 192.175.4.200:3226
Performance stats:
  12899612 output packets
  34508 pkt/s 30s avg, 30495 pkt/s lifetime avg
  14499127648 output Bytes
  38787792 Bps 30s avg, 34276897 Bps lifetime avg
  0 packets lost (retransmits)
  0.00% loss rate 30s avg
  6495624 input packets
  17381 pkt/s 30s avg, 15356 pkt/s lifetime avg
  207859776 input Bytes
  556200 Bps 30s avg, 491394 Bps lifetime avg
FICON performance statistics

You can use the `portShow fcipTunnel` command to view the performance statistics and monitor the behavior of an online FCIP tunnel. This additional information is reported in the details of the command output.

`portshow ficon [Slot/]ge0|ge1 all|tunnel_id [arguments]`

Where:

- `slot` The slot number of a blade in a multi-slot chassis. Does not apply to the 400 Multi-protocol Router.
- `ge0|ge1` The Ethernet port (ge0 or ge1).
- `tunnel_id` Tunnel number (0-7).
- `arguments` are as follows:
  - `globals` General FICON Controls/Statistics.
  - `images` Discovered Images (FCUB).
  - `emul` Emulated FDCBs.
  - `active` Active FDCBs.
  - `epcb` Emulation Control Block (port specific).
  - `fhpb` FICON Host Path Block.
  - `fdpb addr` FICON Device Path Block.
  - `fchb` FICON Channel Control Block.
  - `fcub` FICON Control Unit Control Block.
  - `fdcb addr` FICON Device Control Block.
  - `mem addr` Display 1250 memory in 256 byte increments.
  - `pools` Display current data buffer pool counts.
  - `pmmr` Displays PMMR pointers.
  - `clear` Clears statistics.

The following is an example.

```
Sprint113:root> portshow ficon ge0 all
Port: ge0

VE_STATUS
TunnelId vePort vePortStatus veFeatureBitMap veHashEntryCount
     0 ff     DOWN              0              0
     1 ff     DOWN              0              0
     2 ff     DOWN              0              0
     3 ff     DOWN              0              0
     4 ff     DOWN              0              0
     5 ff     DOWN              0              0
     6 ff     DOWN              0              0
     7 ff     DOWN              0              0

FEATURES
TunnelId XRC TapeWrt TapeRd TinTir DvcLack RdBlkId
     0 OFF     OFF     OFF     OFF     OFF     OFF     OFF
     1 OFF     OFF     OFF     OFF     OFF     OFF     OFF
```
**PARAMETERS**

<table>
<thead>
<tr>
<th>TunnelId</th>
<th>WrtPipe</th>
<th>RdPipe</th>
<th>WrtDevs</th>
<th>RdDevs</th>
<th>WrtTimer</th>
<th>WrtChain</th>
<th>OxidBase</th>
<th>DebugFlags</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000</td>
<td>000</td>
<td>00</td>
<td>00</td>
<td>0000</td>
<td>0000000</td>
<td>0x0000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>1</td>
<td>000</td>
<td>000</td>
<td>00</td>
<td>00</td>
<td>0000</td>
<td>0000000</td>
<td>0x0000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>2</td>
<td>000</td>
<td>000</td>
<td>00</td>
<td>00</td>
<td>0000</td>
<td>0000000</td>
<td>0x0000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>3</td>
<td>000</td>
<td>000</td>
<td>00</td>
<td>00</td>
<td>0000</td>
<td>0000000</td>
<td>0x0000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>4</td>
<td>000</td>
<td>000</td>
<td>00</td>
<td>00</td>
<td>0000</td>
<td>0000000</td>
<td>0x0000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>5</td>
<td>000</td>
<td>000</td>
<td>00</td>
<td>00</td>
<td>0000</td>
<td>0000000</td>
<td>0x0000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>6</td>
<td>000</td>
<td>000</td>
<td>00</td>
<td>00</td>
<td>0000</td>
<td>0000000</td>
<td>0x0000</td>
<td>0x00000000</td>
</tr>
<tr>
<td>7</td>
<td>000</td>
<td>000</td>
<td>00</td>
<td>00</td>
<td>0000</td>
<td>0000000</td>
<td>0x0000</td>
<td>0x00000000</td>
</tr>
</tbody>
</table>

**FTRACE output control and display**

The `portshow ftrace` command can be used to control and display FTRACE output. The capitalized letters in the options represent the minimum set of characters that must be entered. Control arguments that change configuration parameters (such as buffers) are not saved in persistent memory.

**NOTE:** This command is primarily for use by technical support personnel.

```
portShow ftrace [slot/]ge0|ge1 tunnel-id arguments
```

- **slot** Specify the slot number of a blade in a multi-slot chassis.
- **ge0|ge1** The Ethernet port (ge0 or ge1).
- **tunnel-id** Tunnel number (0-7).
- **arguments are as follows.**
  - **ACO on/off** Enable/Disable/Display Auto Check Out.
  - **ACTivate 0-xx** Activate trace 'xx' for viewing.
  - **AScii (8 characters)** Set/reset the ASCII filter.
  - **B** Display the bottom (most recent) trace.
  - **BUFFers n** Specify the number of buffers to configure for a tunnel.
  - **CCfg** Display the current FTRACE configuration.
  - **CI xx / all** Check In trace buffer 'xx', or all buffers.
  - **CO xx / all** Check Out trace buffer 'xx', or all buffers.
  - **COA xx** Check out and activate trace buffer xx.
  - **COMMAND** Set/Reset the FICON command frame filter.
  - **CONFig xx/all** Activate a configuration.
  - **DControl** Set/Reset the FICON device control frame filter.
  - **DISABLE** Disable traces for a tunnel.
  - **DISPlaymask** Set/Display the display mask (0-FFFFFFF).
Enable Enable traces for a tunnel.
Filter Display the active trace filters.
Help Display this menu.
HEX Display traces in HEX.
INDex xx Display traces starting at index 'xx'.
INOxid 0-FFFF Set/Reset the inbound FC OXID filter.
Lcontrol Set/Reset the FICON link control frame filter.
N Display the next trace records.
NCfg Display a new FCTRACE configuration.
OUToxid 0-FFFF Set/Reset the outbound FC OXID filter.
OXid 0-FFFF Set/Reset the inbound and outbound FC OXID filters.
P Display the previous trace record.
PAGE n Set/Display the records per page to display.
PATH Set/Reset the path filter HdHpDdDpChCuDv

Where:
Hd - Hd is the hex value for the Host Domain (the entry domain for this host port into the fabric)
Hp - is the hex value for the Host Port (the entry port of this host connection into the fabric)
Dd - is the hex value for the Device Domain (the entry domain for this device into the fabric)
Dp - is the hex value for the Device Port (the entry port for this device connection into the fabric)
Lp - is the Logical Partition (LPAR) value for the host accessing the specific device. This could also be called CH or FICON Channel Number.
Cu - is the Control Unit number (CUADDR) for the specific FICON connection
Dv - is the Device Number of this FICON connected device.

POST 0-100 Set/Display the post trigger percentage.
Rctl 00-FF Set/Reset the FC R_CTL filter.
RECs Specify/Display the number of records per buffer.
RESET Reset all trace filters.
Rsize Specify the trace record size (80-240 bytes).
RXid 0-FFFF Set/Reset the FC frame RXID filter.
SAVE n Save trace buffer n for a tunnel to non-volatile memory.
SCfg Display the FTRACE configuration saved in persistent storage.
STATS Display the FTRACE stats for a tunnel.
STATUS Set/Reset the FICON status frame filter.
T Display the top (oldest) trace records.
Timestamp Enable/Disable the timestamp display.
TOKEN 0-FFFFFFFF Set/Reset the FICON token filter.
TRAcemask Set/Display the trace mask (0-FFFFFFFF).
TRIGGER Display the first trigger point in the buffer.
TRIGGERMask Set/Display the trigger mask (0-FFFFFFFF).
TRIGGERS Set/Reset the triggered event filter.
TYPE 0-FF Set the FC frame TYPE frame filter.

FC fastwrite concepts

FC fastwrite operates in Fibre Channel network topologies similar to the basic topology shown in Figure 43. FC fastwrite provides accelerated speeds for SCSI Write operations over long distance Fibre
Channel ISLs implemented through the FC-FC Routing Service (FRS) rather than FCIP. FC fastwrite is supported in Fabric OS 5.3.x and later.

Platforms and OS requirements for FC fastwrite

Fabric OS supports FC fastwrite between two 400 Multi-protocol Router or two 4/256 SAN Directors with FR4-18i blades connected by a Fibre Channel network. FC fastwrite is a new feature beginning with Fabric OS release 5.3.0. There is no backwards compatibility with previous releases. Fabric OS 5.3.0 or later is required in the switches/blades at both ends of the FC fastwrite flow to enable this feature.

**NOTE:** FC fastwrite and FCIP tunnels cannot be used on the same 400 Multi-protocol Router or FR4-18i blade.

Constraints for FC fastwrite

Consider the following constraints when configuring FC fastwrite.

- FC fastwrite disables the local Ethernet ports (ge0 and ge1), making it impossible to configure FC fastwrite and FCIP tunnels on the same 400 Multi-protocol Router or FR4-18i blade.
- FC fastwrite does not work in FICON environments.
- FC fastwrite flows may be routed to another 400 Multi-protocol Router or FR4-18i blade on the FC network. This 400 Multi-protocol Router or FR4-18i blade may have active FCIP tunnels over an IP network. FC fastwrite flows may be passed through the FCIP tunnel, but only if the FCIP fastwrite option is disabled on the tunnel.
- FC fastwrite does not support loop device configurations for more than one device.

How FC fastwrite works

FC fastwrite eliminates the latency inherent in sending Transfer Ready back to the initiator when writing data across ISLs to geographically distant target devices. FC fastwrite provides a proxy target (PT) local to the initiator host, and a proxy initiator (PI) local to the target storage device. Figure 44 on page 463 shows how FC fastwrite works.

1. The initiator sends a write command.
2. The PT responds with a Transfer Ready, enabling the host to send more data.
3. The target device processes the write command, and sends a Transfer Ready to solicit more data. The PI intercepts the Transfer Ready, and begins sending data received from the host.
4. The PI continues to stage data received from the initiator, respond locally to Transfer Ready, and send the data to the target device until the target device sends an FCP_RSP.

![Figure 44 How FC fastwrite works](image)

**Figure 44 How FC fastwrite works**

FC fastwrite can improve Write performance. Read performance is unaffected. The gains seen from enabling FC fastwrite depend on several factors, including the following:

- The size of I/O vs. Transfer Ready. In general, the more times a target device sends a Transfer Ready, the greater the performance gain.
- The number of outstanding I/Os (both Write and Read), link speed, and link congestion. FC fastwrite may not result in significant improvement if these factors suggest that the write data is delayed because it is sharing bandwidth.
- Target response latency - If the target is slow in responding to the write command, the data must be held by the remote switch.

**FC fastwrite flow configuration requirements**

FC fastwrite is enabled on both initiator and target ports. There is a possibility where either initiator or target ports may have flows with other devices that do not support FC fastwrite. An FC fastwrite specific zone configuration is used to filter FC fastwrite flows.

**Hardware considerations for FC fastwrite**

FC fastwrite is implemented in a hardware configuration consisting of two 400 Multi-protocol Router or two 4/256 SAN Director or DC Directors with FR4-18i blades connected by Fibre Channel ISLs. Consider the following hardware characteristics and requirements when planning to implement FC fastwrite.

- FC ports on both the 400 Multi-protocol Router and the FR4-18i blade are organized into two groups. Ports 0-7 form one group, and ports 8-15 form the other. A maximum of four ports in each group may be configured as FC fastwrite.
- The maximum bandwidth available for FC fastwrite is 4 Gbps per group. This bandwidth is shared by all write flows.
- Host initiators and target devices must be directly connected to the 400 Multi-protocol Router or FR4-18i blade on their respective ends of the ISL. FC fastwrite must be configured and enabled for the ports on both the ends of the flow. Mismatch of the configuration results in I/O failure.
Configuring and enabling FC fastwrite

The FC-FC (Fibre Channel) Routing Service provides Fibre Channel routing between two or more fabrics without merging those fabrics. The FC-FC Routing Service can be simultaneously used as a Fibre Channel router and for SAN extension over wide area networks (WANs) using FCIP.

Take the following steps to configure and enable FC fastwrite.

1. Create a zone configuration to filter FC fastwrite flows. FC fastwrite flows are configured by creating a zone name with an fcacc token as a prefix. For LSAN configuration, use lsan_fcacc as a prefix, as shown in the following example.

   ```
   #zonecreate fcacc_myzone1, "initiator-wwn; target-wwn"
   #zonecreate LSAN_fcacc_myzone2, "initiator-wwn; target1-wwn; target2-wwn"
   #cfgcreate mycfg, "fcacc_myzone1; LSAN_fcacc_myzone2"
   #cfgenable mycfg
   ```

2. Enable FC fastwrite using the `fastwritecfg` command. Enabling or disabling FC fastwrite with this command disrupts data traffic. For the FR4-18i blade, the command powers the blade off and back on. In the case of the 400 Multi-protocol Router, the switch is rebooted. The process takes up to five minutes.

   ```
   #fastwritecfg --enable slot#
   ```

   Where: slot# is the slot in which the FR4-18i blade is installed. A slot number is not required for the 400 Multi-protocol Router.

   Example:

   ```
   SJ3_6A1_12000_0:root> fastwritecfg --enable 7
   ```

   !!!! WARNING !!!!

   Enabling FC Fastwrite will require powering off and back on the and it may take upto 5 minutes. For non bladed system, the switch will be rebooted. Data traffic will be disrupted.

   Continue (Y,y,N,n): [ n] y

   ```
   SJ3_6A1_12000_0:root> fastwritecfg --disable 7
   ```

   !!!! WARNING !!!!

   Disabling FC Fastwrite will require powering off and back on the and it may take upto 5 minutes. For non bladed system, the switch will be rebooted. Data traffic will be disrupted.

   Continue (Y,y,N,n): [ n] y

   Slot 7 is being powered off

3. Enable FC fastwrite on the ports using the `portcfg` command.

   ```
   #portcfg fastwrite slot#/port_id --enable
   ```

   Where slot# is the slot in which the FR4-18i is installed. A slot number is not required for the 400 Multi-protocol Router.
4. Repeat steps 1 through 3 for the blade or switch on the other end of the FC fastwrite path.
5. Use the `portshow` command to verify that FC fastwrite is enabled.

```
rack1_6a1:root> portshow 3/3
portName: 
portHealth: HEALTHY

Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x20b03       PRESENT ACTIVE F_PORT G_PORT U_PORT
LOGICAL_ONLINE LOGIN NOELP ACCEPT
portType: 10.0
portState: 1 Online
portPhys: 6 In_Sync
portScn: 32 F_Port
port generation number: 0
portId: 022300
portIfId: 43320004
portWwn: 20:23:00:60:69:80:04:8a
portWwn of device(s) connected:
   10:00:00:00:c9:2f:68:4d
Distance: normal
portSpeed: N2Gbps

LE domain: 0
FC Fastwrite: ON
Interrupts: 18 Link_failure: 0 Frjt: 0
Unknown: 0 Loss_of_sync: 2 Fbsy: 0
Lli: 12 Loss_of_sig: 4
Proc_rqrd: 13 Protocol_err: 0
Timed_out: 0 Invalid_word: 0
Rx_flushed: 0 Invalid_crc: 0
Tx_unavail: 0 Delim_err: 0
Free_buffer: 0 Address_err: 0
Overrun: 0 Lr_in: 2
Suspended: 0 Lr_out: 0
Parity_err: 0 Ols_in: 0
2_parity_err: 0 Ols_out: 2
CMI_bus_err: 0

Port part of other ADs: N
```
Disabling FC fastwrite on a blade or switch

Disable FC fastwrite using the `fastwritecfg` command. Disabling FC fastwrite with this command disrupts data traffic. For the FR4-18i blade, the command powers the blade off and back on. In the case of the 400 Multi-protocol Router, the switch is rebooted. The process takes up to five minutes.

```
#fastwritecfg --disable slot#
```

Where `slot#` is the slot in which the FR4-18i blade is installed. A slot number is not required for the 400 Multi-protocol Router.

Example:

```
SJ3_6A1_12000_0:root> fastwritecfg --disable 7

!!!! WARNING !!!!

Disabling FC Fastwrite will require powering off and back on the and it may take upto 5 minutes. For non bladed system, the switch will be rebooted. Data traffic will be disrupted.
Continue (Y,y,N,n): [ n] y

Slot 7 is being powered off
```

Disabling FC fastwrite on a port

To disable FC fastwrite on a port, enter the following command.

```
#portcfg fastwrite slot#/port_id --disable
```

Where `slot#` is the slot in which the FR4-18i is installed, and `port_id` is the port number. A slot number is not required for the 400 Multi-protocol Router.
A Configuring the PID format

Port identifiers (called PIDs) are used by the routing and zoning services in Fibre Channel fabrics to identify ports in the network. All devices in a fabric must use the same PID format, so when you add new equipment to the SAN, you might need to change the PID format on legacy equipment.

**NOTE:** Fabric OS 6.0 only supports PID format 1 (Core PID).

About PIDs and PID binding

The PID is a 24-bit address built from the following three 8-bit fields:

- domain
- area_ID
- AL_PA

Many scenarios cause a device to receive a new PID; for example, unplugging the device from one port and plugging it into a different port as part of fabric maintenance, or changing the Domain ID of a switch, which might be necessary when merging fabrics, or changing compatibility mode settings.

Some device drivers use the PID to map logical disk drives to physical Fibre Channel counterparts. Most drivers can either change PID mappings dynamically, also called *dynamic PID binding*, or use the WWN of the Fibre Channel disk for mapping, also called *WWN binding*.

Some older device drivers behave as if a PID uniquely identifies a device, they use *static PID binding*. These device drivers should be updated, if possible, to use WWN or dynamic PID binding instead, because static PID binding creates problems in many routine maintenance scenarios. Fortunately, very few device drivers still behave this way. Many current device drivers enable you to select static PID binding as well as WWN binding. You should only select static binding if there is a compelling reason, and only after you have evaluated the impact of doing so.

Summary of PID formats

HP switches employ the following types of PID formats:

- **VC encoded**—The format defined by the HP StorageWorks 1Gb series switches. Connections to these switches are not supported in Fabric OS 4.0.0 and later.
- **Native**—Introduced with the HP StorageWorks 2Gb series switches, this format supports up to 16 ports per switch.
- **Core**—Default for the HP StorageWorks 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, SAN Switch 4/32, SAN Switch 4/32B, 4/64 SAN Switch, 400 Multi-protocol Router, Brocade 4Gb SAN Switch for HP p-Class BladeSystem, Brocade 4Gb SAN Switch for HP c-Class BladeSystem, SAN Director 2/128, 4/256 SAN Director, and DC SAN Backbone Director (short name, DC Director). This is the recommended format for HP switches and fabrics. It uses the entire 8-bit address space and directly uses the port number as the area_ID. It supports up to 256 ports per switch.
- **Extended edge**—A format that generates the same PID for a port on switches with 16 ports or less as would native PID format, but also supports up to 256 ports per domain. It should be used only in cases where you cannot upgrade devices to dynamic PID binding and you absolutely cannot reboot your servers. Extended edge PID is supported in Fabric OS 2.6.2 and later, 3.1.2 and later, and 4.2.0 through 5.3.0.

**NOTE:** Extended Edge is not supported on any switch with Fabric OS 6.0 or later.
In addition to the PID formats list here, Interoperability mode supports additional PID formats that are not discussed in this guide.

**Impact of changing the fabric PID format**

If your fabric contains switches that use Native PID, it is recommended that you change the format to Core PID before you add the new, higher port count switches and directors. Also, it is recommended that you use Core PID when upgrading the Fabric OS version on 1Gb and 2Gb series switches.

Depending on your situation, the PID change might or might not entail fabric downtime:

- If you are running dual-fabrics with multipathing software, you can update one fabric at a time without disrupting traffic. Move all traffic onto one fabric in the SAN and update the other fabric. Then move the traffic onto the updated fabric, and update the final fabric.
- Without dual-fabrics, stopping traffic is highly recommended. This is the case for many routine maintenance situations, so dual-fabrics are always recommended for uptime-sensitive environments. If your fabric contains devices that utilize static PID binding, or if you do not have dual-fabrics, you must schedule downtime for the SAN to change the PID format.

**Host reboots**

In some Fibre Channel SAN environments, storage devices and host servers are bound to the host operating system by their PIDs (called their Fibre Channel addresses). In these environments, the hosts and target HBAs in a SAN need to know the full 24-bit PIDs of the hosts and targets they are communicating with, but they do not care how the PIDs are determined. But, if a storage device PID is changed, the host must reestablish a new binding, which requires the host to be rebooted.

With the introduction of the Brocade 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, Brocade 4 Gb SAN Switch for p-Class BladeSystem, SAN Switch 4/32, SAN Switch 4/32B, Core Switch 2/64, SAN Director 2/128, 4/256 SAN Director, and DC SAN Backbone Director (short name, DC Director) the Native PID format used in earlier switches was supplemented with the Core PID format, which is capable of addressing higher port counts. Changing from Native PID format to Core PID format changes the PID, which requires hosts that use port binding to be rebooted.

**Static PID mapping errors**

If you can avoid using drivers that employ static PID binding, you should do so.

With the WWN or dynamic PID binding most typically used with drivers, changing the device’s PID does not affect the PID mapping. However, before updating the PID format, it is necessary to determine whether any devices in the SAN use static PID binding.

For those few drivers that do use static PID binding, changing the PID format breaks the mapping, which must be fixed either by rebooting the host or by using a manual update procedure on the host.

To correct mapping errors caused by static PID binding, see the following sections:

- See “Evaluating the fabric” on page 470 for details on finding devices that use static PID binding. Then see “Online update” on page 472 or “Offline update” on page 473 for recommendations.
- See “Converting port number to area ID” on page 474 for instructions.
Changes to configuration data

Table 101 lists various combinations of before-and-after PID formats, and indicates whether the configuration is affected.

**NOTE:** After changing the fabric PID format, if the change invalidates the configuration data (see Table 101 to determine this), do not download old (pre-PID format change) configuration files to any switch on the fabric.

<table>
<thead>
<tr>
<th>PID format before change</th>
<th>PID format after change</th>
<th>Configuration effect?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Native</td>
<td>Extended Edge</td>
<td>No impact</td>
</tr>
<tr>
<td>Extended Edge</td>
<td>Native</td>
<td>No impact</td>
</tr>
<tr>
<td>Native</td>
<td>Core</td>
<td>You must:</td>
</tr>
<tr>
<td>Core</td>
<td>Native</td>
<td>Reenable zoning, if there is an active zone set and it uses port zones.  You do not need to reconfigure Destination ID (DID) if using:  Performance monitoring  The configure command to change the PID format  The performance monitor database  The zoning database  The DID will be converted by Fabric OS automatically.</td>
</tr>
<tr>
<td>Extended Edge</td>
<td>Core</td>
<td></td>
</tr>
</tbody>
</table>

After changing the fabric PID format and verifying correct fabric operation, resave configuration data by running the `configUpload` command.

Before downgrading firmware, change the PID back to supported PIDs such as Core PID. If the database is automatically converted, save the converted database, and then download the older OS.

Selecting a PID format

All switches in a fabric must use the same PID format, so if you add a switch that uses a different PID format to a fabric, the switch will segment from the fabric. The format you select for your fabric depends on the mix of switches in the fabric, and to an extent on the specific releases of Fabric OS in use (for example, Extended Edge PID format is only available in Fabric OS 2.6.2 and later, Fabric OS 3.1.2 and later, and Fabric OS 4.2.0 through 5.3.0).

If you are building a new fabric with switches running various Fabric OS versions, use Core PID format to simplify port-to-area_ID mapping.

**NOTE:** Switches that are queried using outside calls should be configured using PID 1 (core PID) to ensure that the correct port numbering is used in other management applications.
**Table 102** shows various combinations of existing fabrics, new switches added to those fabrics, and the recommended PID format for that combination. The criteria for the recommendations are first to eliminate host reboots, and second to minimize the need for a host reboot in the future.

### Table 102  PID format recommendations for adding new switches

<table>
<thead>
<tr>
<th>Existing Fabric OS versions; PID format</th>
<th>Switch to be added</th>
<th>Recommendations (in order of preference)</th>
</tr>
</thead>
</table>
| 2.6.2 and later/3.1.2 and later; Native PID | 2.6.2 and later/3.1.2 and later | 1. Use Native PID format for new switch. Host reboot is not required.  
2. Convert existing fabric to Core PID format, upgrading the version of Fabric OS, if necessary. Set Core PID format for new switch. Host reboot is required.  
3. If devices are bound statically and it is not possible to reboot, convert existing fabric to Extended Edge PID format, upgrading the version of Fabric OS, if necessary. Use Extended Edge PID format for new switch. Host reboot is not required. |
| 4.2.0 and later | 2.6.2 and later/3.1.2 and later/4.2.0 and later; Core PID | Use Core PID for new switch. Host reboot is not required. |
| 2.6.2 and later/3.1.2 and later/4.2.0 and later; Extended Edge PID | 2.6.2 and later/3.1.2 and later/6.0 | Change fabric to Core PID. Extended Edge is not supported in Fabric OS 6.0. Host reboot is required. |

### Evaluating the fabric

If there is a possibility that your fabric contains host devices with static PID bindings, you should evaluate the fabric for the following items:

- Find any devices that bind to PIDs.
- Determine how each device driver will respond to the PID format change.
- Determine how any multipathing software will respond to a fabric service interruption.

If current details about the SAN are already available, it might be possible to skip the Data Collection step. If not, it is necessary to collect information about each device in the SAN. Any type of device might be able to bind by PID; each device should be evaluated before attempting an online update. This information has broad applicability, because PID-bound devices are not able to seamlessly perform in many routine maintenance or failure scenarios.
1. Collect device, software, hardware, and configuration data.
   The following is a non-comprehensive list of information to collect:
   • HBA driver versions
   • Fabric OS versions
   • RAID array microcode versions
   • SCSI bridge code versions
   • JBOD drive firmware versions
   • Multipathing software versions
   • HBA time-out values
   • Multipathing software timeout values
   • Kernel timeout values
   • Configuration of switch

2. Make a list of manually configurable PID drivers.
   Some device drivers do not automatically bind by PID, but allow the operator to manually create a PID binding. For example, persistent binding of PIDs to logical drives might be done in many HBA drivers. Make a list of all devices that are configured this way. If manual PID binding is in use, consider changing to WWN binding.
   The following are some of the device types that might be manually configured to bind by PID:
   • HBA drivers (persistent binding)
   • RAID arrays (LUN access control)
   • SCSI bridges (LUN mapping)

3. Analyze data.
   After you have determined the code versions of each device on the fabric, they must be evaluated to find out if any automatically bind by PID. It might be easiest to work with the support providers of these devices to get this information. If this is not possible, you might need to perform empirical testing.
   Binding by PID can create management difficulties in a number of scenarios. It is recommended that you not use drivers that bind by PID. If the current drivers do bind by PID, upgrade to WWN-binding drivers if possible.
   The drivers shipping by default with HP/UX and AIX bind by PID, and so detailed procedures are provided for these operating systems in this chapter. Similar procedures can be developed for other operating systems that run HBA drivers that bind by PID.
   There is no inherent PID binding problem with either AIX or HP/UX. It is the HBA drivers shipping with these operating systems that bind by PID. Both operating systems are expected to release HBA drivers that bind by WWN, and these drivers might already be available through some support channels. Work with the appropriate support provider to find out about driver availability.
   It is also important to understand how multipathing software reacts when one of the two fabrics is taken offline. If the time-outs are set correctly, the failover between fabrics should be transparent to the users. You should use the multipathing software to manually fail a path before starting maintenance on that fabric.

4. Perform empirical testing.
   Empirical testing might be required for some devices, to determine whether they bind by PID. If you are not sure about a device, work with the support provider to create a test environment.
   Create as close a match as practical between the test environment and the production environment, and perform an update using the procedure in “Online update” on page 472.
   Devices that bind by PID are unable to adapt to the new format, and one of three approaches must be taken with them:
   • A plan can be created for working around the device driver’s limitations in such a way as to allow an online update. See the Detailed Procedures section for examples of how this could be done.
   • The device can be upgraded to drivers that do not bind by PID.
   • Downtime can be scheduled to reset the device during the core PID update process, which generally allows the mapping to be rebuilt.
If either of the first two options are used, the procedures should again be validated in the test environment.

Determine the behavior of multipathing software, including but not limited to:
- HBA time-out values
- Multipathing software time-out values
- Kernel time-out values

**Planning the update procedure**

Whether it is best to perform an offline or online update depends on the uptime requirements of the site.

- An offline update must have all devices attached to the fabric be offline.
- With careful planning, it should be safe to update the core PID format parameter in a live, production environment. This requires dual fabrics with multipathing software. Avoid running backups during the update process, as tape drives tend to be very sensitive to I/O interruption. The online update process is only intended for use in uptime-critical dual-fabric environments, with multipathing software (high-uptime environments should always use a redundant fabric SAN architecture). Schedule a time for the update when the least critical traffic is running.

All switches running any version of Fabric OS 3.1.2 and later or 4.2.0 and later are shipped with the Core Switch PID Format enabled, so it is not necessary to perform the PID format change on these switches.

Migrating from manual PID binding (such as persistent binding on an HBA) to manual WWN binding and upgrading drivers to versions that do not bind by PID can often be done before setting the core PID format. This reduces the number of variables in the update process.

**Online update**

The following steps are intended to provide SAN administrators a starting point for creating site-specific procedures.

1. Back up all data and verify backups.
2. Verify that the multipathing software can automatically switch over between fabrics seamlessly. If there is doubt, use the software’s administrative tools to manually disassociate or mark offline all storage devices on the first fabric to be updated.
3. Verify that I/O continues over the other fabric.
4. Disable all switches in the fabric to be updated, one switch at a time, and verify that I/O continues over the other fabric after each switch disable.
5. Change the PID format on each switch in the fabric.
6. Re-enable the switches in the updated fabric one at a time. In a core/edge network, enable the core switches first.
7. After the fabric has reconverged, use the `cfgEnable` command to update zoning.
8. Update the bindings for any devices manually bound by PID. This might involve changing them to the new PIDs, or preferably changing to WWN binding.
    - For any devices automatically bound by PID, two options exist:
      a. Execute a custom procedure to rebuild its device tree online. Examples are provided in the “Converting port number to area ID” on page 474 section of this chapter.
      b. Reboot the device to rebuild the device tree. Some operating systems require a special command to do this, for example “boot –r” in Solaris.
9. For devices that do not bind by PID or have had their PID binding updated, mark online or reassociate the disk devices with the multipathing software and resume I/O over the updated fabric.
10. Repeat with the other fabrics.
Offline update

The following steps are intended to provide SAN administrators a starting point for creating site-specific procedures.

1. Schedule an outage for all devices attached to the fabric.
2. Back up all data and verify backups.
3. Shut down all hosts and storage devices attached to the fabric.
5. Change the PID format on each switch in the fabric.
6. Reenable the switches in the updated fabric one at a time. In a core/edge network, enable the core switches first.
7. After the fabric has reconverged, use the `cfgEnable` command to update zoning.
8. Bring the devices online in the order appropriate to the SAN. This usually involves starting up the storage arrays first, and the hosts last.
9. For any devices manually bound by PID, bring the device back online, but do not start applications. Update their bindings and reboot again if necessary. This might involve changing them to the new PIDs, or might (preferably) involve changing to WWN binding.
10. For any devices automatically bound by PID, reboot the device to rebuild the device tree (some operating systems require a special command to do this, such as “boot –r” in Solaris).
11. For devices that do not bind by PID or have had their PID binding updated, bring them back up and resume I/O.
12. Verify that all I/O has resumed correctly.

Hybrid update

It is possible to combine the online and offline methods for fabrics where only a few devices bind by PID. Because any hybrid procedure is extremely customized, it is necessary to work closely with the SAN service provider in these cases.

Changing to core PID format

In Fabric OS release 4.2.0 and later, Native PID format is not supported; the default format is the Core PID format.

In Fabric OS 3.1.2 and later, Core PID format is the default configuration.

In Fabric OS 2.6.2 and later, Native PID format is the default configuration.

Although the PID format is listed in the configuration file, do not edit the file to change the setting there. Instead, use the `configure` command. When you use the `configure` command, switch databases that contain PID-sensitive information are automatically updated. If you change the setting in the configuration file and then download the edited file, the PID format will be changed, but the database entries will not, and so they will be incorrect.

The following list maps the PID format names to the switch PID address modes used in the management interfaces:

- Native PID—Switch PID address mode 0
- Core PID—Switch PID address mode 1
- Extended edge PID—Switch PID address mode 2
Before changing the PID format, determine if host reboots will be necessary. The section "Host reboots" on page 468 summarizes the situations that may require a reboot.

switch:admin> switchdisable
switch:admin> configure
Configure...

Fabric parameters (yes, y, no, n): [no] y

Domain: (1..239) [1]
BB credit: (1..27) [16]
R_A_TOV: (4000..120000) [10000]
E_D_TOV: (1000..5000) [2000]
WAN_TOV: (1000..120000) [0]
Data field size: (256..2112) [2112]
Sequence Level Switching: (0..1) [0]
Disable Device Probing: (0..1) [0]
Suppress Class F Traffic: (0..1) [0]
SYNC IO mode: (0..1) [0]
Switch PID Address Mode: (0..2) [1] < Set mode number here.
Per-frame Route Priority: (0..1) [0]
Long Distance Fabric: (0..1) [0]

Converting port number to area ID

Except for the following cases, the area ID is equal to the port number:

- When you perform a port swap operation.
- When you enable Extended Edge (also known as “displaced PID”) PID on the director.

If you are using Extended Edge PID format (for example, the 4/256 SAN Director with configuration option 5) and would like to map the output of the port number to the area ID, use the following formula (for ports 0–127):

\[ a = (p + 16) \mod 128 \]

where:

- \( a \) is the area, \( p \) is the port number, \( \mod \) is the modulus (or remainder)

\( 0 \leq p < 128 \)

When the port number is greater than or equal to 128, the area ID and port number are the same. Figure 45 shows a 4/256 SAN Director with Extended Edge PID.
Figure 45 4/256 SAN Director with extended edge PID
Performing PID format changes

There are several routine maintenance procedures which might result in a device receiving a new PID. Examples include, but are not limited to:

- Changing compatibility mode settings
- Changing switch Domain IDs
- Merging fabrics
- Relocating devices to new ports or new switches (that is, for Add, Move, Change type operations)
- Updating the core PID format
- Using hot spare switch ports to deal with failures

In every case where devices employ static PID binding, any such procedure becomes difficult or impossible to execute without downtime.

In some cases, device drivers allow you to specify static PID binding. In these cases, such devices must be identified and their PID binding should be changed to WWN binding.

Basic procedure

The following sections contain a basic procedure that summarizes the steps necessary to perform PID format changes without disrupting the fabric, and special procedures for HP/UX and AIX.

This process should be executed as part of the overall online or offline update process. However, it can be implemented in a standalone manner on a non-production fabric, or a switch that has not yet joined a fabric.

1. Ensure that all switches in the fabric are running one of the minimum Fabric OS versions listed below that support the addressing mode:
   - 2Gb series switches—2.6.2
   - SAN Switch 2/8EL and SAN Switch 2/16—3.1.2
   - SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, Core Switch 2/64, SAN Director 2/128—4.2.0
   - Brocade 4 Gb SAN Switch for p-Class BladeSystem—5.0.0
   - Brocade 4/8 SAN Switch, 4/16 SAN Switch, 4/256 SAN Director—5.0.1
   - 4/64 SAN Switch, 400 Multi-protocol Router or 4/256 SAN Director with an FR4-18i blade—5.1.0

   **NOTE:** All switches running any version of Fabric OS 4.0.0 and later are shipped with the Core Switch PID Format enabled, so it is not necessary to perform the PID format change on these switches.

2. Telnet into one of the switches in the fabric.
3. Enter the `switchDisable` command to disable the switch.
4. Enter the `configure` command (the configure prompts display sequentially).
5. Enter `y` after the “Fabric parameters” prompt.
6. Enter `1` at the “Core Switch PID Format” prompt.
7. Respond to the remaining prompts or press `Ctrl-d` to accept the remaining settings without responding to all the prompts.
8. Repeat steps 2 through 7 for the remaining switches in the fabric.
9. Enter the `switchEnable` command to re-enable the switch. For example:

```
switch:admin> switchdisable
switch:admin> configure
Configure...
   Fabric parameters (yes, y, no, n): [no] yes
   Domain: (1..239) [1]
   R_A_TOV: (4000..120000) [10000]
   E_D_TOV: (1000..5000) [2000]
   Data field size: (256..2112) [2112]
   Sequence Level Switching: (0..1) [0]
   Disable Device Probing: (0..1) [0]
   Suppress Class F Traffic: (0..1) [0]
   SYNC IO mode: (0..1) [0]
   Core Switch PID Format: (0..2) [0] 1
   Per-frame Route Priority: (0..1) [0]
   Long Distance Fabric: (0..1) [0]
   BB credit: (1..27) [16]
```

10. After all switches are updated to use the new PID format and re-enabled, verify the fabric has fully reconverged (each switch "sees" the other switches).

11. Enter `cfgEnable [active_zoning_config]` on one of the switches in the fabric to update zoning to use the new PID form. This does not change the definition of zones in the fabric; it causes the lowest level tables in the zoning database to be updated with the new PID format setting. It is only necessary to do this once per fabric; the zoning update automatically propagates to all switches.

At this point, all switches in the fabric are operating in the new addressing mode.

### HP/UX procedure

This procedure is not intended to be comprehensive. It provides a starting point from which a SAN administrator could develop a site-specific procedure for a device that binds automatically by PID, and cannot be rebooted due to uptime requirements.

1. Back up all data. Verify backups.
2. If you are not using multipathing software, stop all I/O going to all volumes connected through the switch and fabric to be updated.
3. If you are not using multipathing software, unmount the volumes from their mount points using `umount`. The proper usage is `umount <mount_point>`. For example:

```
umount /mnt/jbod
```
4. If you are using multipathing software, use that software to remove one fabric’s devices from its configuration.
5. Deactivate the appropriate volume groups using `vgchange`. The proper usage is `vgchange -a n <path_to_volume_group>`. For example:

```
vgchange -a n /dev/jbod
```
6. Make a backup copy of the volume group directory using `tar` from within `/dev`. For example:

```
tar -cf /tmp/jbod.tar jbod
```
7. Export the volume group using `vgexport`. The proper usage would be `vgexport -m <mapfile> <path_to_volume_group>`. For example:

```
vgexport -m /tmp/jbod_map /dev/jbod
```
8. Connect to each switch in the fabric.
9. Issue the `switchDisable` command.
10. Issue the `configure` command and change the Core Switch PID Format to 1.
11. Issue the command `cfgEnable [effective_zone_configuration]`. For example:

```
cfgEnable my_zones
```
12. Issue the `switchEnable` command. Enable the core switches first, then the edges.
13. Clean the `lvmtab` file with the command `vgscan`.

Fabric OS 6.x administrator guide 477
14. Change to /dev and untar the file that was tared in step 4. For example:
   `tar -xf /tmp/jbod.tar`

15. Import the volume groups using vgimport. The proper usage would be
   `vgimport -m <mapfile> <path_to_volume_group> <physical_volume_path>`. For example:
   `vgimport -m /tmp/jbod_map /dev/jbod /dev/dsk/c64t8d0 /dev/dsk/c64t9d0`

16. Activate the volume groups using vgchange. The proper usage would be `vgchange -a y <path_to_volume_group>`. For example:
   `vgexport -a y /dev/jbod`

17. If you are not using multipathing software, mount all devices again and restart I/O. For example:
   `mount /mnt/jbod`

18. If you are using multipathing software, reenable the affected path. The preceding steps do not “clean up” the results from ioscan. When viewing the output of ioscan, notice the that the original entry is still there, but now has a status of NO_HW.

   # ioscan -funC disk
   
<table>
<thead>
<tr>
<th>Class</th>
<th>I H/W Path</th>
<th>Driver S/W State H/W Type Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk</td>
<td>0 0/0/1/1.2.0</td>
<td>adisk CLAIMED DEVICE SEAGATE ST39204LC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/dev/dsk/clt2d0 /dev/rdsk/clt2d0</td>
</tr>
<tr>
<td>disk</td>
<td>1 0/0/2/1.2.0</td>
<td>adisk CLAIMED DEVICE HP DVD-ROM 304</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/dev/dsk/c3t2d0 /dev/rdsk/c3t2d0</td>
</tr>
<tr>
<td>disk</td>
<td>319 0/4/0.1.2.255.14.8.0</td>
<td>adisk CLAIMED DEVICE SEAGATE ST336605FC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/dev/dsk/c64t8d0 /dev/rdsk/c64t8d0</td>
</tr>
<tr>
<td>disk</td>
<td>320 0/4/0.1.18.255.14.8.0</td>
<td>adisk NO_HW DEVICE SEAGATE ST336605FC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/dev/dsk/c65t8d0 /dev/rdsk/c65t8d0</td>
</tr>
</tbody>
</table>

19. Remove the original (outdated) entry. The proper usage for this command is `rmsf -a -v <path_to_device>`. For example:
   `rmsf -a -v /dev/dsk/c65t8d0`

20. Enter the `ioscan -funC disk` command to validate that the entry has been removed. In this example, the NO_HW entry is no longer listed:

   het46 (HP-50001)> ioscan -funC disk

<table>
<thead>
<tr>
<th>Class</th>
<th>I H/W Path</th>
<th>Driver S/W State H/W Type Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk</td>
<td>0 0/0/1/1.2.0</td>
<td>adisk CLAIMED DEVICE SEAGATE ST39204LC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/dev/dsk/clt2d0 /dev/rdsk/clt2d0</td>
</tr>
<tr>
<td>disk</td>
<td>1 0/0/2/1.2.0</td>
<td>adisk CLAIMED DEVICE HP DVD-ROM 304</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/dev/dsk/c3t2d0 /dev/rdsk/c3t2d0</td>
</tr>
<tr>
<td>disk</td>
<td>319 0/4/0.1.2.255.14.8.0</td>
<td>adisk CLAIMED DEVICE SEAGATE ST336605FC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/dev/dsk/c64t8d0 /dev/rdsk/c64t8d0</td>
</tr>
</tbody>
</table>

21. Repeat for all fabrics.

22. Issue the `switchEnable` command. Enable the core switches first, then the edges.
AIX procedure

This procedure is not intended to be comprehensive. It provides a starting point from which a SAN administrator can develop a site-specific procedure for a device that binds automatically by PID, and cannot be rebooted due to uptime requirements.

1. Back up all data. Verify backups.
2. If you are not using multipathing software, stop all I/O going to all volumes connected through the switch or fabric to be updated.
3. If you are not using multipathing software, vary the volume groups offline. The command usage is `varyoffvg <volume_group_name>`. For example:
   ```bash
   varyoffvg dataavg
   ```
4. If you are not using multipathing software, unmount the volumes from their mount points using `umount`. The command usage is `umount <mount_point>`. For example:
   ```bash
   umount /mnt/jbod
   ```
5. If you are using multipathing software, use that software to remove one fabric’s devices from its configuration.
6. Remove the device entries for the fabric you are migrating. For example, if the HBA for that fabric is `fcs0`, execute the command:
   ```bash
   rmdev -Rdl fcs0
   ```
7. Connect to each switch in the fabric.
8. Issue the `switchDisable` command.
9. Issue the `configure` command and change the Core Switch PID Format to 1.
10. Issue the `configEnable [effective_zone_configuration]` command. For example:
    ```bash
    configenable my_config
    ```
11. Issue the `switchEnable` command. Enable the core switches first, then the edges.
12. Rebuild the device entries for the affected fabric using the `cfgMgr` command. For example:
    ```bash
    cfgmgr -v
    ```
    This command might take several minutes to complete.
13. If you are not using multipathing software, vary the disk volume groups online. The proper usage would be `varyonvg <volume_group_name>`. For example:
    ```bash
    varyonvg dataavg
    ```
14. If you are not using multipathing software, mount all devices again and restart I/O. For example:
    ```bash
    mount /mnt/jbod
    ```
15. If you are using multipathing software, reenable the affected path.
16. Repeat all steps for all fabrics.
Swapping port area IDs

If a device that uses port binding is connected to a port that fails, you can use port swapping to make another physical port use the same PID as the failed port. The device can then be plugged into the new port without the need to reboot the device.

Use the following procedure to swap the port area IDs of two physical switch ports. In order to swap port area IDs, the port swap feature must be enabled, and both switch ports must be disabled. The swapped area IDs for the two ports remain persistent across reboots, power cycles, and failovers.

**4/256 SAN Director and DC SAN Backbone Director (short name, DC Director) only:** You can swap only ports 0 through 15 on the FC4-48 and FC8-48 port blade. You cannot swap ports 16 through 47.

To swap area IDs for a pair of switch ports:

1. Connect to the switch and log in as admin.
2. Enable the port swap feature:
   ```
   portswapenable
   ```
3. **HP StorageWorks 4/8, 4/16, 4/32, 4/32B, 4/64, Brocade 4 Gb SAN Switch for p-Class BladeSystem, Brocade 4 Gb SAN Switch for c-Class BladeSystem, and 400 Multi-protocol Router switches:** Enter the following commands:
   ```
   portdisable port1
   portdisable port2
   ```

4. **4/256 SAN Director and DC SAN Backbone Director (short name, DC Director):** Enter the following commands:
   ```
   portdisable slot/port1
   portdisable slot/port2
   ```

4. **HP StorageWorks 4/8, 4/16, 4/32 and 400 Multi-protocol Router switches:** Enter the following command:
   ```
   portswap port1 port2
   ```

5. **4/256 SAN Director and DC SAN Backbone Director (short name, DC Director):** Enter the following command:
   ```
   portswap slot1/port1 slot2/port2
   ```

6. Verify that the port area IDs have been swapped:
   ```
   portswapshow
   ```
   A table is shows the physical port numbers and the logical area IDs for any swapped ports.

7. Disable the port swap feature:
   ```
   portswapdisable
   ```
B Implementing an interoperable fabric

This appendix provides information on setting up a heterogeneous fabric that includes Fabric OS switches and McDATA Enterprise OS switches (M-EOS).

**IMPORTANT:** These features are not supported at the time of the release of this document. Please check with your sales representative or [http://www.hp.com](http://www.hp.com) regarding HP support of the interoperability features.

In Fabric OS 6.0, Brocade supports interoperability on new platforms, zone activation, FCR SANtegrity, Fabric OS SANtegrity, and Coordinated Hot Code Load.

Prior to this release, you could configure switches for interoperability mode (Open Fabric 1.0), by enabling interopmode 1, which supported non-Brocade switches, for example CISCO and QLogic. This release introduces McDATA Open Fabric mode, interopmode 3, which replaces interopmode 1. You can configure interoperability between McDATA and Brocade switches, but interoperability on non-Brocade switches is no longer supported.

McDATA Open Fabric mode is intended specifically for adding Fabric OS-based products into M-EOS fabrics that are already using Open Fabric mode. Fabrics containing only Fabric OS switches in Open Fabric mode are not supported.

McDATA switch firmware must run version 9.6.2 to support interoperability. All Fabric OS switches must run version 6.0.

Overview

Changing the interop mode is no longer a toggle operation. The `interopmode` command allows changing between McDATA Fabric, McDATA Open Fabric, and back to Brocade Native mode. You must issue the `interopmode` command on all Fabric OS switches in the fabric and all switches must have the same mode set. All fabric mode changes can only be performed when the switch is disabled or offline and any platform management functions must be disabled. You no longer have to perform a reboot, each Fabric OS switch automatically reboots when you change modes.

Fabric OS 6.0 supports changing between interop modes using the following `Interopmode` command options:

- `Interopmode 2` for McDATA Fabric mode supports M-EOS switches v9.6.2 and later running in McDATA Fabric mode.
- `Interopmode 3` for McDATA Open Fabric mode supports M-EOS switches v9.6.2 and higher running in Open Fabric mode.
- `Interopmode 0` for Brocade Native mode, which supports all stand alone Brocade fabrics, but no interoperability support.

Understanding Brocade and McDATA interoperability

Determining McDATA-aware features

There are two ways that Fabric OS 6.0 determines which features are available to the switch. If a feature is McDATA-aware (that is, aware of the McDATA environment), some actions may be possible fabric-wide. If a feature is McDATA-unaware, some actions cannot be taken.

Features that are available fabric-wide in a McDATA-aware environment are shown in Table 103.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coordinated Hot Code Load</td>
<td>Supported McDATA Open Fabric mode and McDATA Fabric mode.</td>
</tr>
<tr>
<td>FCR E_Port SANtegrity</td>
<td>Supported only in McDATA Fabric mode.</td>
</tr>
</tbody>
</table>
Implementing an interoperable fabric

Determining McDATA-unaware features

Features that are unaware of McDATA switches or fabrics and cannot be used fabric-wide are shown in Table 104.

Table 104  McDATA-unaware features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware download</td>
<td>Supported on Fabric OS 6.0 switches.</td>
</tr>
</tbody>
</table>

Security

- Secure Fabric OS                  | Not supported.                   |
- ACL in strict mode                 | Not supported.                   |
- ACL in non-strict (Tolerant) mode, Absent mode, and others (such as password authentication) | Supported. |
- Admin Domains                      | Not supported.                   |
- FICON and FICON CUP                | Not supported.                   |
- Fabric-wide diagnostics (FC-Ping, PathInfo) | Not supported.                   |
Supported Connectivity for Fabric 6.0

Brocade switches can directly connect to the following Brocade M-series (formerly McDATA) directors: Mi10k, M6140, M6064 and switches: 4700, 4400, 4500, 4300, 3232, 3216, 3032, 3016.

Other M-EOS 9.6.2 products can reside in the same fabric as a Brocade switch but cannot directly connect to it. M-EOS 9.6.2 must be running on all Fibre Channel switches in the fabric.

The Multi protocol Router, and the Brocade FR4-18i blade can connect to a Brocade switch for routing between fabrics.

HP StorageWorks blade server SAN switch modules and switches can connect to the fabric using the Access Gateway feature.

Figure 46 Typical configuration

Feature support and interoperability

Table 105 is a comprehensive matrix of feature support. Some features are discussed in detail in later sections.

Table 105 Complete feature compatibility matrix

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>• ACL in strict mode: No</td>
<td>Works in conjunctions with SANegrity.</td>
</tr>
<tr>
<td></td>
<td>• ACL in tolerant mode: Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ACL in absent mode: Yes</td>
<td></td>
</tr>
<tr>
<td>Admin Domains</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Advanced Performance</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Beaconsing</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Compatibility</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Config Download/Upload</td>
<td>Yes</td>
<td>Displays the credit number in the <code>configure</code> command.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Environmental Monitor</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Error Event Management</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Extended Fabrics</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Fabric Device Management Interface (FDMI)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Fabric Watch</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>FICON (includes CUP)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>High Availability</td>
<td>Yes</td>
<td>HCL (Hot Code Load) in Fabric OS 6.0</td>
</tr>
<tr>
<td>Interoperability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fabric OS Native Mode</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>McDATA Open Mode</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>McDATA Fabric Mode</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>IP over FC</td>
<td>Yes</td>
<td>Works on a local HP switch. Broadcast frames are sent to F_Ports only; there is no forwarding of broadcast frames to E_Ports.</td>
</tr>
<tr>
<td>License</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Log Tracking</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Management Server</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Manufacturing Diagnostics</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>N_Port ID Virtualization</td>
<td>Yes</td>
<td>The tested limits for NPIV are 24 NPIV channels x 12 virtual port logins.</td>
</tr>
<tr>
<td>Name Server</td>
<td>Yes</td>
<td>Support Domain offset, McDATA specific SWRSCN, FCFG commands (GE_PT, GSNN_NN, GSPN_ID, and GA_NXT).</td>
</tr>
<tr>
<td>Network Time Protocol (NTP)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Open E_Port</td>
<td>Yes</td>
<td>Autonegotiates the R_RDY mode by default. Uses &quot;portcfgislmode&quot; to static configure the port.</td>
</tr>
<tr>
<td>Port mirroring</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Secure Fabric OS</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>SNMP</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
M-EOS 9.6.2 features supported in Fabric OS 6.0

In addition to support for McDATA Fabric mode, Fabric OS 6.0 supports other M-EOS 9.6.2 feature capabilities. Some features have inherent limitations. These are described here.

Port number offset

Some M-EOS switches assign PIDs with an area field (the middle byte of the PID) that has an offset of four added to the port number. This means, for example, that the physical port number 0 has an address value used in the PID of 4.

The port number offset is conveyed between the neighboring switches through the ESS ILS (Exchange Security Attributes), allowing neighboring switches to accurately identify port numbers and their associated PIDs. The maximum port number is also available in the ESS ILS.

NPIV

NPIV management on switch running 6.0 is the same as in the standard Fabric OS.
Trunking

HP switches support trunking when participating in an M-EOS Native fabric. Trunk ports (bandwidth aggregation) only apply to ISL between two HP switches.

**NOTE:** Trunking is allowed between Brocade switches in Native mode only. Trunking is disabled between Brocade switches running in McDATA Open Fabric mode.

- **Fabric OS frame-based trunking** is supported for frame-based ISLs. Multiple ISLs between a Brocade switch and an M-EOS type switch are allowed, but no frame-based trunking will occur.
- **Fabric OS exchange-level trunking** (DPS) and **source-port route balancing** (DLS) are supported for connections between Brocade switches and M-EOS switches.
- **M-EOS Open Trunking** is supported for outbound ISLs from any M-EOS switch to any switch in the fabric.

**M-EOS 9.6.2 features not supported by Fabric OS 6.0**

**Domain ID offset configuration**

Domain ID offset is used by McDATA switches in assigning the first byte of the PID for attached end devices. McDATA Fabric mode supports a Domain ID range from 1 to 31 and McDATA Open Fabric mode supports a Domain ID range of 97-127; the starting offset of this range of Domain IDs can be modified. The offset value, which can be any multiple of 0x20 up through 0xC0, is added to the actual Domain ID of the switch and is used in assigning the PID. Traditionally, M-EOS based switches used an offset of 0x60, or 96 in decimal notation. For example, a switch with a Domain ID configured to 3 would assign a value of 99 (0x63) to the first byte of all PIDs.

HP StorageWorks switches do not support Domain ID offset configuration, and requires the default 0x60 (96) offset value.

**Diagnostic test differences**

The diagnostic tests `porttest` and `spinfab` are designed to work with an E_Port linked to Brocade-attached switches. These diagnostics will fail if the E_Port is linked to a McDATA switch.

**Optional 6.0 licensing**

The following optional licensed features are available and supported with Fabric OS 6.0:

**Table 106  Supported optional features**

<table>
<thead>
<tr>
<th>License</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports on Demand</td>
<td>Provision additional ports through license key upgrade.</td>
</tr>
<tr>
<td>Extended Fabrics</td>
<td>Allows up to 500 km of switched-fabric connectivity at full bandwidth over long distances.</td>
</tr>
<tr>
<td>Fabric Watch</td>
<td>Monitors mission-critical switch operations.</td>
</tr>
<tr>
<td>ISL Trunking Over Extended Fabrics</td>
<td>ISL Trunking has been enhanced to enable trunking over long distance links up to 250 km through a new command—LD (variable distance). This feature will only work when forming trunks between a Brocade and McDATA switch in the fabric.</td>
</tr>
</tbody>
</table>
The following licensed features are not supported with Fabric OS 6.0:

Table 107  Unsupported features

<table>
<thead>
<tr>
<th>License</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Zoning</td>
<td>In Fabric OS 6.0, Advance zoning does require a license. Zoning is configured through M-EOS switches.</td>
</tr>
<tr>
<td>Fabric Manager</td>
<td>Enables administration, configuration, and maintenance of fabric switches and SANs with host-based software. Only supports Brocade switches.</td>
</tr>
<tr>
<td>Advanced Performance</td>
<td>Monitoring Enables performance monitoring of networked storage resources.</td>
</tr>
</tbody>
</table>

Supported switches

The following matrix identifies the hardware platforms that are included in this releases.

Table 108  Fabric OS Interoperability with M-EOS

<table>
<thead>
<tr>
<th>McDATA Fabric mode</th>
<th>Fabric OS 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>NI Support</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chassis Type</th>
<th>Blade Type</th>
<th>McDATA Open Fabric and Fabric Mode NI Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/256 SAN Director</td>
<td>16/32/48 port -4G</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>10G</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>16/32/48 port -8G</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>FC4-16IP</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>FR4-18i</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>FA4-18</td>
<td>Yes</td>
</tr>
<tr>
<td>DC SAN Backbone Director</td>
<td>16/32/48 -8G</td>
<td>No</td>
</tr>
<tr>
<td>(short name, DC Director)</td>
<td>10G</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>FC4-16IP</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>FR418i</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>FA4-18</td>
<td>No</td>
</tr>
</tbody>
</table>

Switches and Appliances

<table>
<thead>
<tr>
<th>Multi-protocol Router</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/8 SAN Switch or 4/16 SAN Switch</td>
<td>Yes</td>
</tr>
<tr>
<td>Embedded Server Blades</td>
<td>Yes</td>
</tr>
<tr>
<td>SAN Switch 4/32B</td>
<td>Yes</td>
</tr>
<tr>
<td>4/64 SAN Switch</td>
<td>Yes</td>
</tr>
<tr>
<td>SAN Switch 4/32</td>
<td>No</td>
</tr>
</tbody>
</table>
Supported features McDATA Fabric mode (interopmode 2)

The following features are supported in Fabric OS 6.0:

- Zone activation
  Zoning managed through EFCM
- ESA frame support
- Coordinated Hot Code Load
- FCR E_Port SANtegrity
- Fabric OS L2 SANtegrity Support
- No limitations on the number of E_Port connections to any Brocade switch
- HA support for zoning

Supported features McDATA Open Fabric mode (interopmode 3)

The following features are supported in Fabric OS 6.0:

- Coordinated Hot Code Load
- HA support for zoning
- No limitations on the number of E_Port connections to any Brocade switch
- Fabric Watch

Unsupported features McDATA Fabric and Open Fabric modes

The following optional features are not supported and cannot be installed on any Fabric OS switch in the fabric:

- Extended PID mode format
- Quickloop and QuickLoop Zoning
- Secure Fabric OS
- Timer Server function
- Open E_Port
- Broadcast Zoning
- Management Server Service and FDMI
- QuickLoop Fabric Assist
- Remote Switch
- Extended Fabrics
- Alias Server
- Platform Service
- FCIP
- FICON

McDATA Fabric mode configuration restrictions

- Maximum 2048 devices.
- Extended Edge PID format cannot be used.
- Maximum 31 switch (Domain ID) limitation.
- Domain IDs must be in the 1 to 31 value range on Fabric OS switches for successful connection to McDATA switches. The firmware automatically assigns a valid Domain ID, if necessary.
- The DCC policy or port based security is not supported in McDATA Fabric mode.
- The `msplMgmtDeactivate` command must be run prior to connecting the Brocade switch to a McDATA switch to de-activate any platform management functions because McDATA switches do not understand Brocade proprietary frames used to exchange platform information.
McDATA Open Fabric mode configuration restrictions

- Maximum 200 devices.
- Maximum 4 switch (Domain ID) limitation.
- Domain IDs must be in the 97 to 127 value range on Fabric OS switches for successful connection to McDATA switches. The firmware automatically assigns a valid Domain ID, if necessary. If Fabric OS 6.0 is installed on a Brocade switch, and when McDATA Open Fabric is enabled on the switch, then from a McDATA perspective, 97-127 appear as 1-31.
- Does not support domain, port zoning, or default zoning.
- Does not support McDATA SANtegrity feature.
- No Zone activations or zoning management.
- No support for Brocade proprietary features.
- The `msplMgmtDeactivate` command must be run prior to connecting the Brocade switch to a McDATA switch to deactivate any platform management functions because McDATA switches do not understand Brocade proprietary frames used to exchange platform information.

Upgrade and downgrade restrictions

- Brocade only supports one version upgrades and downgrades, for example if you have Fabric OS 5.2.0 installed, you must upgrade to Fabric OS 5.3.0 only before upgrading to Fabric OS 6.0.
- In McDATA Fabric mode - Fabric OS 5.2.1_NI is the on Fabric OS version that can upgrade directly to Fabric OS 6.0.

Zoning restrictions

Zone activation is only supported in McDATA Fabric mode. It allows you to create new zone configurations or modify enabled zone configurations, which can be activated as the enabled zone configuration from McDATA or Brocade switches. You can save these configurations to the defined Database on the local Brocade switch. Zone activation allows fabric-wide and stand alone activation of zone configuration. Before creating or configuring a zone, see the following zone requirements for McDATA Fabric mode:

- A zoning license and a fabric license must be installed on each Fabric OS switch.
- There are four zoning limits that must be met:
  - Maximum Number of Zones – 2047 (+1 for the default zone)
  - Maximum Number of Member per Zone – 4096
  - Maximum Number of Unique Zone Members per Zone Set – 4096
  - Maximum Zone Set Definition Size – 0x32000
  - No support in the FCR Backbone
- Only zoning by port WWN is allowed; you must use the port WWN of the device, such as 10:00:00:00:c9:28:c7:c6.
- Zone members specified by node WWN are ignored.
- When a Brocade switch or director is reconfiguring, wait until the fabric routes are completely set up before entering zoning commands that must propagate to other switches. Use the `fabricShow` command to verify that all fabric routes are set up and all switch IP addresses and names are present. (The `fabricShow` command only shows the WWN and Domain ID for switches from other manufacturers.)
- When no zoning configuration is in effect, and without Default Zoning enabled on McDATA by default, all ports are isolated and traffic is not permitted. This is unlike Brocade behavior with Brocade Native mode enabled (and all data traffic is enabled). If the default zone is disabled and there is no active configuration, then no device can communicate with any other device in the fabric if zoning has been disabled on a Brocade switch. For details, see “Activating Default Zones” in “Administering Advanced Zoning” on page 403.
- Allows you to define zones in the effective configuration or the Defined Database.
- The `Cfgenable` and `cfgdisable` commands activate the effective zone configuration.
• Brocade switches connected to McDATA switches receive the effective configuration when a zone merge occurs. (McDATA only has an effective zone configuration and discards the defined zone configuration when it sends merge information to the Brocade switch.) However, a zone update sends the defined and effective configuration to all switches in the fabric.

• Use the `cfgsaveactivetodefined` command to move the effective configuration to the defined configuration database.

• Legacy McDATA switches do not support the Defined Database or merge propagation.

• `Cfgsiz` checks the maximum available size and the currently saved size of the zoning configuration. If you believe you are approaching the maximum, you can save a partially completed zoning configuration and re-issue the `cfgsize` command to determine the remaining space.

• Supports fabric-wide activation of zone configurations.

• New CLI command `cfgmcdtmode` to activate and deactivate McDATA Default and Safe Zoning features.

• Allows Domain Port number zoning. Zone configurations that use either physical port numbers or port IDs are supported.

• Zone database is managed on the EFCM Management Server.

• New `cfgsaveactivetodefined` command moves the current effective configuration to the Defined database.

• `Cfgsave` only saves the Defined Database on the local switch; Defined Database distribution is not supported.

Zone name restrictions

The name field must contain the ASCII characters that actually specify the name, not including any required fill bytes. Names must follow these rules:

• Length must be between 1 and 64 characters.

• All characters must be 7-bit ASCII.

• The first character must be a letter, which can be either upper case (A-Z) or lower case (a-z).

• Any character other than the first character must be lower case (a-z), upper case (A-Z), a single-digit number (0-9), dash (-), or underscore (_).

• McDATA Fabric mode allows the characters dash (-), caret (^) and dollar sign ($) in zone names.

Activating zones in McDATA Fabric mode

Activating zones mean creating zone configurations on legacy McDATA switches. McDATA Default Zone and McDATA Safe Zone replace Brocade Default zoning. You can activate McDATA Default Zone or McDATA Safe Zone, but not both. Activating the default zone enables any device in the default zone to see any other device in the default zone. If the default zone is disabled and no zones are active, then devices connected to the switch are unable to communicate.

Default zone

A default zone consists of all devices that are not members of a zone in a currently enabled (active) zone set. If a zone set is active, then all connected devices that are not included in at least one of the zones in the active zone set are included in the default zone. You can enable or disable the default zone separately from the active zone set. If no zone set is enabled, then all devices are considered to be in the default zone.

Default zoning adds devices not explicitly zoned to a default “catch-all” zone in M-EOS 9.6.2 Fabrics. When a device is added to a configured zone, it is automatically removed from the default zone. Default zoning is fabric-wide and is exchanged during E Port initialization between adjacent switches. After the E Port initialization, if zoning is changed, the update is propagated throughout the fabric through a standard zone update.
Safe zone

Safe zoning is a fabric-wide parameter that ensures that the resulting zone set of two merged fabrics is consistent with the pre-merged zone sets. When you enable Safe zone, the Default Zone must be disabled and the zoning configuration of neighboring switches must match completely before the zoning can merge.

To allow a Brocade switch into an M-EOS Native fabric, safe zoning must be disabled. This allows the Brocade switch to join the fabric although the zone sets do not match. After the fabric merge and zone merge are completed, safe zoning may be re-enabled.

Activating zone configurations on a standalone switch

To activate zone configurations on a standalone switch:

1. Connect to the switch and log in as admin.
2. Enter the `interopmode` command with the appropriate option to activate the zone, for example:

   ```
   InteropMode [0|2|3 [-z McDataDefaultZone] [-s McDataSafeZone]]
   0: to turn interopMode off
   2: to turn McData Fabric mode on
   Valid McDatatDefaultZone: 0 (disabled), 1 (enabled)
   Valid McDataSafeZone: 0 (disabled), 1 (enabled)
   3: to turn McDATA Open Fabric mode on
   ```

Activating zone configurations fabric-wide

To activate zoning fabric-wide:

1. Connect to the switch and log in as admin.
2. Enter the `cfgmcdtmode` command with the appropriate option, for example

   ```
   cfgmcdtmode [--enable | --disable | --help] [safezoning | defaultzoning]
   ```

   ```
   cfgmcdtmode --enable safezoning
   safezoning McDATA mode has been enabled ...
   ```

**NOTE:** The `interopmode` and `cfgMcdtmode` commands perform the same functions. The `interopmode` command only affects the local configuration and the command must be issued on each switch in the fabric. The `cfgMcdtmode` affects the entire fabric.

Verifying the effective zone configuration

An effective zone configuration is a subset of the defined zone configuration, containing only the zone configuration objects that are currently enabled; only one configuration can be active at a time, but multiple configurations can be defined in the database. You must verify that the active zone set or zone configuration has correctly propagated to the other switches in the fabric. You can enter the `cfgenable` command with the name of the zone configuration to activate the effective zone configuration and the `cfgdisable` command with the name of the zone configuration to deactivate the effective zone configuration.

When uploading and downloading configuration files, you must be sure that the file being moved contains the correct information. After a configuration is committed, any inaccurate parameters must be manually corrected.

In McDATA Fabric mode, you can set the effective zone configuration to the Defined Database. If the Defined Database contains a configuration with the same name, it will be replaced. Any non-duplicate zone sets or zones will remain unchanged. Before moving the effective zone configuration to the Defined Database, you should view the zoning configuration.
To view zoning configurations:

- Enter the `cfgShow` command to view the zoning configuration.

```
switch:admin> cfgShow
Default Zone: OFF
Safe Zone: OFF
Defined configuration:
cfg: switch set
  switch1; switch2; switch3; switch4
zone: switch1
[output truncated]
...
Effective configuration:
cfg: switch set
zone: switch1
  12,64
[output truncated]
```

To save the effective zone configuration to the defined database:

The defined database is not synchronized between Brocade switches in McDATA Fabric mode. When you create a zone configuration on one switch, the new configuration is not synchronized to the defined database. You must save the configuration to synchronize it to the defined database.

- Enter the `cfgSaveActiveToDefined` command.

```
switch:admin> cfgSaveActiveToDefined
You are about to save the Defined zoning configuration. This action will save the effective configuration to the defined configuration.
Do you want the Effective zoning to become the Defined zoning? (yes, y, no, n): [no] yes
Attempting to save new config to the defined config...
2sw0 Updating flash ...
...
[output truncated]
...
Attempting to save config to the defined config...
2sw0 Updating flash ...

Updating flash ...
```
Moving to McDATA Open Fabric mode from earlier Fabric OS versions

To move from interopmode 1 under Fabric OS 5.3 to Open Fabric mode:

1. Enter the `switchDisable` command to disable the switch.
   `switch:admin> switchdisable`
2. Enter the `interopmode 0` command (native Brocade mode).
3. Upgrade to Fabric OS 6.0.
4. Enter the `interopmode 3` command to configure the switch to Open Fabric mode.
5. After the automatic reboot, the switch will be online, establish ISL connection(s) to Open Fabric mode.

Enabling McDATA Open Fabric mode

When configuring McDATA Open Fabric mode, avoid Domain ID conflicts before fabric reconfiguration. When configuring multiple switches, you should wait for a fabric reconfiguration after adding or removing each switch. Every switch in the fabric must have a unique Domain ID.

To enable McDATA Open Fabric mode:

1. Verify that you have implemented all the Brocade prerequisites necessary to enable `interopmode 3` on the fabric (see “McDATA Open Fabric mode configuration restrictions” on page 489.)
2. Connect to the switch and log in as `admin`.
   Ensure that the switch is disabled or offline.
3. Enter the `switchDisable` command to disable the switch.
   `switch:admin> switchdisable`
4. Enter the `configure` command to set the Domain ID to a number in the range from 97 to 127; otherwise, the `interopmode` command will default you to 97. For detailed instructions, see “Working with domain IDs” on page 16.
   `switch:admin> configure`
   Configure...
   Fabric Parameters (yes, y, no, n): [no] y
   Domain (1...127): [1] 97
5. Enter the `interopmode 3` command to enable interoperability. This command resets a number of parameters and enables McDATA Open Fabric mode.
   `switch:admin> interopmode 3`
   McDATA Open Fabric mode is enabled
   The switch effective configuration will be lost.
   The system will reboot to allow the change to take effect.
   Do you want to continue? (yes, y, no, n): [no] y
   The configuration is being saved - a system reboot will cause the change to take effect.
   Please disable switch before changing the interop mode.

   The switch automatically reboots after changing the interoperability mode.
6. Repeat step 2 through step 5 on each Brocade switch in the fabric. For more information on the switch, refer to the switch documentation.
7. After enabling McDATA Open Fabric mode on all switches, physically connect the legacy McDATA switches to the Brocade fabric, one at a time.
Enabling McDATA Fabric mode

When McDATA Fabric mode is turned on, the OUI portion of the switch WWN is no longer replaced with a McDATA OUI. All existing zoning configurations will be cleared.

To enable McDATA Fabric mode

1. Verify that you have implemented all the Brocade prerequisites necessary to enable `interopmode 2` on the fabric (see “McDATA Fabric mode configuration restrictions” on page 488.)

2. Connect to the switch and log in as admin.
   Ensure that the switch is disabled or offline.

3. Enter the `switchDisable` command to disable the switch.
   
   switch:admin> `switchdisable`

4. Enter the `configure` command to set the Domain ID to a number in the range from 97 to 127. (For detailed instructions, see “Working with domain IDs” on page 36.)
   
   switch:admin> `configure`
   
   Configure...
   
   Fabric Parameters (yes, y, no, n): [no] `y`
   
   Domain (1...127): [1] `97`

5. Enter the `interopmode 2` command to enable interoperability. This command resets a number of parameters and enables fabric mode.
   
   switch:admin> `interopmode 2`
   
   McDATA Fabric mode is enabled
   
   The switch effective configuration will be lost.
   The system will reboot to allow the change to take effect.
   Do you want to continue? (yes, y, no, n): [no] `y`
   
   The configuration is being saved - a system reboot will cause the change to take effect.
   Please disable switch before changing the interop mode.

   The switch automatically reboots after changing the interoperability mode.

6. Repeat step 2 through step 5 on each Brocade switch in the fabric. For more information on the switch, refer to the switch documentation.

7. After enabling McDATA Fabric mode on all switches, physically connect the legacy McDATA switches to the Brocade fabric, one at a time.
Enabling Brocade Native mode

When you change the mode from McDATA Fabric or McDATA Open Fabric mode to Brocade Native mode, existing configurations will be erased and the switch must assume the zone configuration from the fabric it joins or a new configuration must be configured. When you change the switch to Brocade Native mode, all configuration parameters return to their default states and can be modified using the configure command. The existing preferred configuration must be changed to a value within the user Domain ID range specified for the mode before changing to Brocade Native mode is allowed. If the preferred Domain ID is not in this range, the mode conversion changes the Domain ID to 1.

To enable Brocade Native mode or disable interoperability:

1. Connect to the switch and log in as admin.
2. Enter the `switchDisable` command to disable the switch.
   ```
   switch:admin> switchdisable
   ```
3. Enter the `interopmode 0` command to disable interoperability.
   ```
   switch:admin> interopmode 0
   Interop mode is disabled
   The switch effective configuration will be lost.
   The system will reboot to allow the change to take effect.
   Do you want to continue? (yes, y, no, n): [no] y
   ```
4. The switch reboots automatically after changing the interoperability mode.
5. After removing each switch, wait for a fabric reconfiguration.
6. Repeat this procedure on all Brocade switches in the fabric.

**NOTE:** McDATA switches cannot talk to switches in Brocade Native mode.

Enabling Fabric OS L2 SANtegrity (Fabric Binding)

SANtegrity is required only in legacy McDATA fabrics running EFCM management software. The support for SANtegrity in this release is for Fabric Binding. Fabric Binding is required for FICON in mixed fabrics. Fabric OS 6.0 will run separate fabric security policies that will be analogous to SANtegrity fabric binding. Interaction between McDATA SANtegrity and Fabric OS security policies is minimized to McDATA SANtegrity requests initiated by the attached McDATA switch. Brocade security policies do not initiate any requests or verifications to the McDATA fabric. Downgrading to a Fabric OS version that does not support SANtegrity interoperability without first disabling Fabric Binding will cause ports to segment upon subsequent initialization (for example, disable and then enable or add new ISL).

When Fabric Binding is turned on, only the switches that are currently in the fabric are included in the binding list that is sent out.

Fabric Binding lets you configure a Fabric Binding Membership list that each switch in a fabric can use to validate between itself and its neighbor. McDATA SANtegrity Fabric Binding uses a list made up of Domain ID and WWN pairs and implies Insistent Domain IDs. Brocade uses Fabric Data Distribution of Switch Connection Control policies through a Brocade fabric. Interoperability between mixed fabrics requires switches to exchange and validate their Fabric Binding Membership list upon bringing up an ISL. When Fabric Binding is enabled, a Fabric Binding check is performed each time a link is initialized to ensure that the switches can connect. If this check fails on either switch, the link will be segmented.

EFCM software facilitates the synchronization of the Brocade and McDATA policies and should be used to configure and enable Fabric Binding in a mixed fabric. Configuration through other management interfaces requires careful synchronization, and is not recommended.

Fabric Binding is always enabled or disabled on the entire fabric. EFCM allows enabling Fabric Binding either separately or as part of the Enterprise Fabric mode feature. Enterprise Fabric mode is used for FICON environments and turns on several features including Fabric Binding.
NOTE: Turning off McDATA Enterprise Fabric mode does NOT turn off any of the features that it turned on.

Enabling Fabric Binding using EFCM will automatically enable Insistent Domain ID on all Fabric OS and McDATA switches in the fabric. Disabling Fabric Binding does not turn off Insistent Domain ID.

EFCM automates the Fabric Binding configuration process.

**FCR SANtegrity (Fabric Binding)**

The support for FCR SANtegrity in this release is for Fabric Binding. FCR Fabric Binding is for use with EX_Ports attached to a McDATA edge switch. It is strongly recommended to use EFCM to configure and enable or disable Fabric Binding. Downgrading to a Fabric OS version that does not support SANtegrity interoperability without first disabling Fabric Binding will cause ports to segment upon subsequent initialization (for example, disable and then enable or add new ISL).

Fabric Binding lets you configure a Fabric Binding Membership list that each switch in a fabric can use to validate between it and its neighbor. McDATA SANtegrity Fabric Binding uses a list made up of Domain ID and WWN pairs and implies Insistent Domain IDs. When Fabric Binding is enabled, a Fabric Binding check is performed each time a link is enabled to ensure that the switches can connect. If the binding check fails, the McDATA port will go to an invalid attachment state and the FCR EX_Port will disable itself.

NOTE: After a Fabric Binding check failure between a McDATA E_Port and FCR EX_port, the current McDATA implementation requires you to disable the McDATA port and then re-enable it before the link can come up again. Enabling just the FCR EX_Port will not allow the link to come up again.

Brocade FCR implements a simplified version of Fabric Binding that is passive and only checks whether its own Front Port Domain ID and WWN pair is present in the Fabric Binding list that is sent from a McDATA switch.

Translate domains behind the Front Port Domain must be handled in the following manner:

- Translate domains that are already present before Fabric Binding is enabled must be included in the Fabric Binding List created using EFCM.
- Translate domains that are created after Fabric Binding is enabled do not have to be added to the Fabric Binding List and do not cause any Fabric Binding checks to fail. If Fabric Binding is subsequently disabled, these translate domains must be added to the Fabric Binding List before Fabric Binding can be re-enabled.
- Translate domains do not have Insistent Domain ID behavior.

**Enabling FCR Fabric Binding**

Fabric Binding is always enabled or disabled on the entire fabric. EFCM allows enabling Fabric Binding either separately or as part of the Enterprise Fabric mode feature. Enterprise Fabric mode is used for FICON environments and turns on several features including Fabric Binding.

NOTE: Turning off McDATA Enterprise Fabric mode does NOT turn off any of the features that it turned on.

Unlike L2 SANtegrity, FCR requires additional configuration using Brocade CLI before configuring and enabling Fabric Binding using EFCM.

The McDATA Fabric Binding uses a list made up of Domain ID and WWN pairs. Because the FCR front port WWN cannot be predetermined, you must connect the FCR to the McDATA edge switch before the Fabric Binding List can be filled in with the FCR front port Domain ID and WWN entry.
1. On the FCR, enter the `portcfgexport` command to configure the preferred Domain ID. This preferred Domain ID will become Insistent whenever Fabric Binding is enabled. If the port is not already set to McDATA Fabric mode, this command may also be used to set it.

2. Enable the EX_Ports configured in the previous step.

3. Use EFCM to create the Fabric Binding list and to enable Fabric Binding.

**NOTE:** The front port preferred Domain ID will behave as insistent while Fabric Binding is enabled. Fabric Binding must be disabled prior to removing an EX_Port from a bound fabric to disable the Insistent Domain ID behavior on that EX_Port. Failure to do this will result in Insistent Domain ID behavior of the EX_Port even if it is subsequently connected to an edge fabric that is not using Fabric Binding.

---

**Support for coordinated Hot Code Load**

Fabric OS 6.0 supports non-disruptive Hot Code load (HCL) on all Fabric OS single-CP switches when connected to a mixed fabric with McDATA switches running in either McDATA Fabric or McDATA Open Fabric mode. Hot Code is only guaranteed if all switches in an Interop fabric support the new protocol. This feature eliminates the need to automatically configure E_Ports with large number of BB_Credits in mixed fabrics. This also removes the limit for the number of E_Ports that can be supported. All switches in the fabric must run version M-ESO 9.6.2 to guarantee a non-disruptive code load sequence. Coordinated Hot Code Load provides:

- Fabric-wide pause and resume
- No limitations on E_Port count or fabric membership
- Flood pause frame to all switches in the fabric before initiating a reboot

Fabric OS running on single CP switches takes approximately 60 seconds to restart as part of the code upload process. During the time when the Fabric OS switch software is unavailable, with the uninterrupted data traffic, M-EOS switches and directors in the same fabric send point-to-point frames (Hello, LSU) and domain controller frames (GEPT) to the Fabric OS switch.

Fabric OS 6.0 notifies all switches in the fabric about a pending Hot Code activation (or HA-boot) so that they can stop sending control frames to the specified switch until it restarts and sends a resume notification. When a switch initiates a graceful shutdown sequence to prepare for Hot Code load, it can flood a notification frame to all supported switches in the fabric.

Information added to the ESS indicates which switches support the new protocol. The receiving (remote) switches responds to the notification by suppressing both Fabric Controller and Domain Controller frames to the Hot Code switch. After the restart completes, the Hot Code switch must flood a resume traffic notification message to all supported switches.

**Supported configurations**

All switches in the fabric must support the defined protocol. Non-disruptive Hot Code is supported on any fabric configuration and mix of switches.

Hot Code load is supported on the following platforms:

- EOS-support for all M-EOS based Directors and switches
- All Fabric OS 6.0 supported platforms

HCL does not affect Director Class products because of their fast switch-over capability

**Upgrade and downgrade considerations**

Table 109 lists upgrade and downgrade considerations from either McDATA Fabric mode or Open mode. It does not consider upgrades or downgrades from Brocade Native mode.
### Activating Hot Code Load

1. Enter the `firmwaredownload` command without any option. `firmwaredownload` checks whether all switches in the fabric support HCL. If HCL is supported, `firmwaredownload` proceeds and displays the normal message. If HCL is not supported, `firmwaredownload` fails and prompts you to use the `-o` option. `firmwaredownload` is not running at that point.

2. Enter `firmwaredownload -o`. `firmwaredownload` does not check whether all switches in the fabric support HCL. If the normal checks are successful, it proceeds and displays the normal message plus an additional message. The `firmwaredownload -o` command upgrades both CPs in the switch. If you want to upgrade a single CP only, use the `-s` option.

   You can run `firmwaredownloadstatus` to get the status of this `firmwaredownload`.

   The `firmwaredownload -o` command causes a warm and nondisruptive boot on the active CP, but requires that existing Telnet, Secure Telnet, or SSH sessions be restarted.

   You have elected to bypass the checking of Coordinated HCL. This may cause traffic disruption for some switches in the fabric.

   Do you want to proceed?

   If you select **yes**, `firmwaredownload` proceeds and failure of the pause protocol is ignored.

---

**Table 109  Hot Code upgrade considerations**

<table>
<thead>
<tr>
<th>Fabric OS Versions</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Upgrading from any other down-level release | • Must upgrade to Brocade Native mode, and then change the interopmode; cannot be in McDATA Open Fabric mode before the upgrade.  
  • The upgrade is disruptive or has the potential to be disruptive. |
| Upgrade to higher release than Fabric OS 6.0 or Patch release of Fabric OS 6.0 | • Will be nondisruptive |
## C Understanding legacy password behavior

This appendix provides password information for early versions of Fabric OS firmware.

### Password management information

Table 110 describes the password standards and behaviors between various versions of firmware.

<table>
<thead>
<tr>
<th>Topic</th>
<th>4.0.0</th>
<th>4.1.0 to 4.2.0</th>
<th>4.4.0 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of default accounts on the switch</td>
<td>4, chassis-based</td>
<td>Core Switch 2/64 · 8 for the director, 4 per switch. All other switches and directors · 4</td>
<td>Core Switch 2/64 · 8 for the director, 4 per switch. All other switches and directors · 4</td>
</tr>
<tr>
<td>Default account names</td>
<td>root, factory, admin, user</td>
<td>root, factory, admin, user</td>
<td>root, factory, admin, user</td>
</tr>
<tr>
<td>Account name changing feature</td>
<td>No</td>
<td>No, regardless of security mode.</td>
<td>supports the userRename command</td>
</tr>
<tr>
<td>Maximum and minimum number of characters for a password</td>
<td>0 · 8 (Standard UNIX)</td>
<td>8 · 40 characters with printable ASCII</td>
<td>8 · 40 characters with printable ASCII</td>
</tr>
<tr>
<td>Can different switch instances use a different password for the same account login level? For example, the password for admin for switch 0 can be different from password for admin for switch 1.</td>
<td>No</td>
<td>Yes for Core Switch 2/64. n/a for all other switches.</td>
<td>Yes for Core Switch 2/64. n/a for all other switches.</td>
</tr>
<tr>
<td>Does the root account use restricted shell?</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>When connecting to a factory installed switch, do you use the default passwords?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Does a user need to know the old passwords when changing passwords using the passwd command?</td>
<td>Yes, except when the root user changes another user’s password. This is standard UNIX behavior; Fabric OS does not enforce any additional security.</td>
<td>Old password is required only when changing password for the same level user password. Changing password for lower level user does not require old password. For example, users connect as admin; old admin password is required to change the admin password. But old user password is not required to change the user password.</td>
<td>4.4.0 to 5.1.0 only: Old password is required only when changing password for the same level user password. Changing password for lower level user does not require old password. For example, users connect as admin; old admin password is required to change the admin password. But old user password is not required to change the user password.</td>
</tr>
</tbody>
</table>
### Table 111: Password prompting matrix

<table>
<thead>
<tr>
<th>Topic</th>
<th>4.0.0</th>
<th>4.1.0 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must all password prompts be completed for any change to take effect?</td>
<td>No. Partial changes of all four passwords are allowed.</td>
<td>No. Partial changes of all four passwords are allowed.</td>
</tr>
<tr>
<td>When does the password prompt appear?</td>
<td>When users connect as root, factory, or admin, the accounts with default password will be prompted for change. The accounts with non-default password will NOT be prompted.</td>
<td>When users connect as root, factory, or admin, the accounts with default password will be prompted for change. The accounts with non-default password will NOT be prompted.</td>
</tr>
<tr>
<td>Is a user forced to answer password prompts before getting access to the firmware?</td>
<td>No, users can type in Ctrl-c to get out of password prompting.</td>
<td>No, users can type in Ctrl-c to get out of password prompting.</td>
</tr>
<tr>
<td>Do users need to know the old root password when answering prompting?</td>
<td>Yes in 4.0.0</td>
<td>No</td>
</tr>
<tr>
<td>Are new passwords forced to be set to something different than the old passwords?</td>
<td>Yes in 4.0.0</td>
<td>Yes</td>
</tr>
<tr>
<td>Is password prompting disabled when security mode is enabled?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Is the <code>passwd</code> command disabled until the user has answered password prompting?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Does password prompting reappear when passwords are changed back to the default using the <code>passwd</code> command?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Does password prompting reappear when passwords are changed back to the default using the <code>passwdDefault</code> command?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Password migration during firmware changes

Table 112 describes the expected outcome of password settings when upgrading or downgrading firmware for various Fabric OS versions.

Table 112  Password migration behavior during firmware upgrade/downgrade

<table>
<thead>
<tr>
<th>Topic</th>
<th>4.4.0 to 5.0.1</th>
<th>5.0.1 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords used when upgrading to a newer firmware release for the first time.</td>
<td>Default accounts and passwords are preserved.</td>
<td>Default accounts and passwords are preserved.</td>
</tr>
<tr>
<td>Passwords preserved during subsequent firmware upgrades</td>
<td>Multi-user accounts created during a previous upgrade to 5.0 are restored.</td>
<td>Multi-user accounts created during a previous upgrade to 5.1.0 are restored.</td>
</tr>
<tr>
<td>Passwords used if downgrading to an earlier firmware for the first time</td>
<td>Downgrades to 4.4.0 preserve all existing default accounts, multi-user accounts and passwords. Multi-user accounts with the switchAdmin role have the same permissions as the user role.</td>
<td>Downgrades to 5.0.1 preserve all existing default accounts, multi-user accounts and passwords.</td>
</tr>
<tr>
<td>When downgrading to an earlier firmware at subsequent times, which passwords will be used?</td>
<td>Downgrades to 4.4.0 preserve all existing default accounts, multi-user accounts and passwords. Multi-user accounts with the switchAdmin role have the same permissions as the user role.</td>
<td>Downgrades to 5.0.1 preserve all existing default accounts, multi-user accounts and passwords.</td>
</tr>
<tr>
<td>When downgrading then upgrading again, what passwords will be used?</td>
<td>All default and multi-user accounts and passwords remain unchanged.</td>
<td>All default and multi-user accounts and passwords remain unchanged.</td>
</tr>
</tbody>
</table>

Password recovery options

Table 113 describes the options available when one or more types of passwords are lost.

Table 113  Password recovery options

<table>
<thead>
<tr>
<th>Topic</th>
<th>4.0.0</th>
<th>4.1.0 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>If all the passwords are forgotten, what is the password recovery mechanism? Are these procedures non-disruptive recovery procedures?</td>
<td>Contact HP. A non-disruptive procedure is available.</td>
<td>Contact HP. A non-disruptive procedure is available.</td>
</tr>
<tr>
<td>If a user has only the root password, what is the password recovery mechanism?</td>
<td>Root can change any password by using the passwd command.</td>
<td>Use passwd command to set other passwords. Use passwdDefault command to set all passwords to default.</td>
</tr>
<tr>
<td>How to recover boot PROM password?</td>
<td>n/a</td>
<td>Contact HP and provide the recovery string. Refer to “Boot PROM password” on page 78 for more information.</td>
</tr>
<tr>
<td>How do I recover a user, admin, or factory password?</td>
<td>Contact HP. Refer to “Recovering forgotten passwords” on page 82 for more information.</td>
<td>Contact HP. Refer to “Recovering forgotten passwords” on page 82 for more information.</td>
</tr>
</tbody>
</table>
D  Using Remote Switch

This appendix provides information on the Remote Switch feature.

About Remote Switch

The Remote Switch feature, which aids in ensuring gateway compatibility, was formerly a licensed feature. Its functionality is now available as part of the Fabric OS standard feature set through the use of the `portCfgIslMode` command, which is described in “Linking through a gateway” on page 44. For those who use Remote Switch as part of their legacy set of tools, this appendix contains a description and procedure for the feature.

Remote Switch enables you to connect two remote HP switches over an IP network, enabling communication of IP or ATM protocols as well as Fibre Channel traffic.

The Remote Switch feature functions with the aid of a “bridging device” or Fibre Channel gateway. The gateway supports both a Fibre Channel physical interface and a secondary, non-Fibre Channel physical interface, such as IP, SONET, or ATM. Remote Switch functions over E_Port connections. With Remote Switch on both fabrics, the gateway accepts Fibre Channel frames from one fabric, tunnels them across the network, and passes them to the other fabric. From the viewpoint of the connected hosts and storage devices, fabrics using Remote Switch interact the same as locally connected switches.

Remote Switch capabilities

Remote Switch provides many of the same capabilities of normal ISL links including the following:

- Coordinated fabric services
  The Remote Switch fabric configuration fully supports all fabric services, including distributed name service, registered state change notification, and alias service.

- Distributed management
  Management tools such as Advanced Web Tools, Fabric OS, and SNMP are available from both the local switch and the remote switch. Switch management is routed through the Fibre Channel connection; thus, no additional network connection is required between sites.

- Support for interswitch links (ISLs)
  Sites requiring redundant configurations can connect multiple E_Ports to remote sites by using multiple gateways. Standard Fabric OS routing facilities automatically maximize throughput and provide automatic failover during interruption on the WAN connection.

Using Remote Switch with a gateway

The Remote Switch feature operates in conjunction with a gateway. The gateway provides an E_Port interface that links to the HP StorageWorks switch E_Port. After the link between the two E_Ports has been negotiated, the gateway E_Port moves to passthrough mode and passes Fibre Channel traffic from the switch E_Port to the WAN.

The gateway accepts Fibre Channel frames from one side of a Remote Switch fabric, transfers them across a WAN, and passes them to the other side of the Remote Switch fabric.

Remote Switch can be used for the following types of gateway devices:

- Fibre Channel over ATM
- Fibre Channel over IP
- Fibre Channel over SONET
- Fibre Channel over DWDM

Most of these gateway devices have enough buffers to cover data transfer over a wide area network (WAN). The HP StorageWorks switches on each side of the gateway must have identical configurations. Only qualified SFPs should be used.

You must connect the fabrics through the gateway device, and make sure that the `configure` parameters are compatible with the gateway device.
You may be required to reconfigure the following parameters, depending on the gateway requirements:

**NOTE:** Consult your gateway vendor for supported and qualified configurations.

- **R_A_TOV:** Specify a Resource Allocation Timeout Value compatible with your gateway device.
- **E_D_TOV:** Specify an Error Detect Timeout Value compatible with your gateway device.
- **Data field size:** Specify the maximum Fibre Channel data field reported by the fabric. Verify the maximum data field size the network-bridge can handle. Some bridges may not be able to handle a maximum data field size of 2112.
- **BB credit:** Specify the number of Buffer-to-Buffer credits for Nx_Port devices.
- **Suppress Class F Traffic:** Use this parameter to disable class F traffic. Some network-bridge devices may not have a provision for handling class F frames. In this case, the transmission of class F frames must be suppressed throughout the entire Remote Switch fabric.

To set the access and reconfigure these parameters:

1. Connect to the switch and log in as admin.
2. Enter the `switchdisable` command to disable the switch.
3. Enter the `configure` command.
4. At the Fabric Parameters prompt enter `yes`.
5. Press Enter to scroll through the Fabric Parameters without changing their values, until you reach the parameter you want to modify.
6. Specify a new parameter value that is compatible with your gateway device.
7. Press Enter to scroll through the remainder of the configuration parameters. Make sure that the configuration changes are committed to the switch.
8. Repeat for all switches in the fabrics to be connected through a gateway device. These parameters must be identical on each switch in the fabric, and between fabrics connected through the gateway device.

This example shows how to modify the data field size and suppress class F traffic on a switch:

```
switch:admin> switchdisable
switch:admin> configure
Configure...
Fabric parameters (yes, y, no, n): [no] yes
Domain: (1..239) [3]
    R_A_TOV: (4000..120000) [10000]
    E_D_TOV: (1000..5000) [2000]
    Data field size: (256..2112) [2112] 1000
    Sequence Level Switching: (0..1) [0]
    Disable Device Probing: (0..1) [0]
    Suppress Class F Traffic: (0..1) [0] 1
    VC Encoded Address Mode: (0..1) [0]
    Per-frame Route Priority: (0..1) [0]
    Long Distance Fabric: (0..1) [0]
    BB credit: (1..16) [16]
Virtual Channel parameters (yes, y, no, n): [no]
    Zoning Operation parameters (yes, y, no, n): [no]
    RSCN Transmission Mode (yes, y, no, n): [no]
    NS Operation Parameters (yes, y, no, n): [no]
    Arbitrated Loop parameters (yes, y, no, n): [no]
    System services (yes, y, no, n): [no]
    Portlog events enable (yes, y, no, n): [no]
Committing configuration...done.
switch:admin>
```
## Zone merging scenarios

Table 114 provides information on merging zones and the expected results.

### Table 114 Zone merging scenarios

<table>
<thead>
<tr>
<th>Description</th>
<th>Switch A</th>
<th>Switch B</th>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Switch A</strong> has a defined configuration.</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: none</td>
<td>defined: none effective: none</td>
<td>Configuration from <strong>Switch A</strong> to propagate throughout the fabric in an inactive state, because the configuration is not enabled.</td>
</tr>
<tr>
<td><strong>Switch B</strong> does not have a defined configuration.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Switch A</strong> has a defined and enabled configuration.</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: cfg1:</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: none</td>
<td>Configuration from <strong>Switch A</strong> to propagate throughout the fabric. The configuration is enabled after the merge in the fabric.</td>
</tr>
<tr>
<td><strong>Switch B</strong> has a defined configuration but no effective configuration.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Switch A</strong> and <strong>Switch B</strong> have the same defined configuration. Neither have an enabled configuration.</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: none</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: none</td>
<td>No change (clean merge).</td>
</tr>
<tr>
<td><strong>Switch A</strong> and <strong>Switch B</strong> have the same defined and enabled configuration.</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: cfg1:</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: cfg1:</td>
<td>No change (clean merge).</td>
</tr>
<tr>
<td><strong>Switch A</strong> does not have a defined configuration. <strong>Switch B</strong> has a defined configuration.</td>
<td></td>
<td></td>
<td><strong>Switch A</strong> will absorb the configuration from the fabric.</td>
</tr>
<tr>
<td><strong>Switch A</strong> does not have a defined configuration. <strong>Switch B</strong> has a defined configuration.</td>
<td>defined: none effective: none</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: none</td>
<td><strong>Switch A</strong> will absorb the configuration from the fabric, with cfg1 as the effective configuration.</td>
</tr>
<tr>
<td><strong>Switch A</strong> does not have a defined configuration. <strong>Switch B</strong> has a defined configuration.</td>
<td>defined: none effective: none</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: cfg1</td>
<td><strong>Switch A</strong> will absorb the configuration from the fabric, with cfg1 as the effective configuration.</td>
</tr>
<tr>
<td><strong>Switch A</strong> and <strong>Switch B</strong> have the same defined configuration. Only <strong>Switch B</strong> has an enabled configuration.</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: none</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: cfg1</td>
<td>Clean merge, with cfg1 as the effective configuration.</td>
</tr>
<tr>
<td><strong>Switch A</strong> and <strong>Switch B</strong> have different defined configurations. Neither have an enabled zone configuration.</td>
<td>defined: cfg2: zone2: ali3; ali4 effective: none</td>
<td></td>
<td>Clean merge. The new configuration will be a composite of the two. defined: cfg1: zone1: ali1; ali2 cfg2: zone2: ali3; ali4 effective: none</td>
</tr>
<tr>
<td><strong>Switch A</strong> and <strong>Switch B</strong> have different defined configurations. <strong>Switch B</strong> has an enabled configuration.</td>
<td>defined: cfg2: zone2: ali3; ali4 effective: none</td>
<td>defined: cfg1: zone1: ali1; ali2 effective: cfg1</td>
<td>Clean merge. The new configuration will be a composite of the two, with cfg1 as the effective configuration.</td>
</tr>
</tbody>
</table>
### Table 114 Zone merging scenarios (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Switch A</th>
<th>Switch B</th>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective configuration mismatch.</td>
<td>defined: cfg1 zone1: ali1; ali2 effective: cfg1 zone1: ali1; ali2</td>
<td>defined: cfg2 zone2: ali3; ali4 effective: cfg2 zone2: ali3; ali4</td>
<td>Fabric segments due to: Zone Conflict cfg mismatch</td>
</tr>
<tr>
<td>Configuration content mismatch.</td>
<td>defined: cfg1 zone1: ali1; ali2 effective: irrelevant</td>
<td>defined: cfg1 zone1: ali3; ali4 effective: irrelevant</td>
<td>Fabric segments due to: Zone Conflict content mismatch</td>
</tr>
<tr>
<td>Same content, different effective cfg name.</td>
<td>defined: cfg1 zone1: ali1; ali2 effective: cfg1 zone1: ali1; ali2</td>
<td>defined: cfg2 zone1: ali1; ali2 effective: irrelevant</td>
<td>Fabric segments due to: Zone Conflict cfg mismatch</td>
</tr>
<tr>
<td>Same content, different zone name.</td>
<td>defined: cfg1 zone1: ali1; ali2 effective: irrelevant</td>
<td>defined: cfg1 zone1: ali2; ali1 effective: irrelevant</td>
<td>Fabric segments due to: Zone Conflict content mismatch</td>
</tr>
<tr>
<td>Same content, different alias name.</td>
<td>defined: cfg1 ali1: A; B effective: irrelevant</td>
<td>defined: cfg1 ali2: A; B effective: irrelevant</td>
<td>Fabric segments due to: Zone Conflict content mismatch</td>
</tr>
<tr>
<td>Same alias name, same content, different order.</td>
<td>defined: cfg1 ali1: A; B effective: irrelevant</td>
<td>defined: cfg1 ali1: B; C effective: irrelevant</td>
<td>Fabric segments due to: Zone Conflict content mismatch</td>
</tr>
<tr>
<td>Same name, different types.</td>
<td>effective: zone1: MARKETING</td>
<td>effective: cfg1: MARKETING</td>
<td>Fabric segments due to: Zone Conflict type mismatch</td>
</tr>
<tr>
<td>Same name, different types.</td>
<td>effective: zone1: MARKETING</td>
<td>effective: alias1: MARKETING</td>
<td>Fabric segments due to: Zone Conflict type mismatch</td>
</tr>
<tr>
<td>Same name, different types.</td>
<td>effective: cfg1: MARKETING</td>
<td>effective: alias1: MARKETING</td>
<td>Fabric segments due to: Zone Conflict type mismatch</td>
</tr>
<tr>
<td><strong>Switch A</strong> does not have Traffic Isolation (TI) zones.</td>
<td>defined: cfg1 TI_zone1</td>
<td>defined: cfg1</td>
<td>Clean merge.</td>
</tr>
<tr>
<td><strong>Switch A</strong> has TI zones.</td>
<td>defined: cfg1 TI_zone1</td>
<td>defined: cfg1 TI_zone1</td>
<td>Clean merge.</td>
</tr>
<tr>
<td><strong>Switch B</strong> has TI zones.</td>
<td>defined: cfg1 TI_zone1</td>
<td>defined: cfg1 TI_zone2</td>
<td>Fabric segments due to: Zone Conflict cfg mismatch. Cannot merge switches with different TI zone configurations.</td>
</tr>
<tr>
<td><strong>Switch A</strong> has a TI zone.</td>
<td>defined: cfg1 TI_zone1</td>
<td>defined: cfg1 TI_zone2</td>
<td>Fabric segments due to: Zone Conflict cfg mismatch. Cannot merge switches with different TI zone configurations.</td>
</tr>
<tr>
<td><strong>Switch B</strong> has a different TI zone.</td>
<td>defined: cfg1 TI_zone1</td>
<td>defined: cfg1 TI_zone2</td>
<td>Fabric segments due to: Zone Conflict cfg mismatch. Cannot merge switches with different TI zone configurations.</td>
</tr>
<tr>
<td>Different default zone access mode settings.</td>
<td>defzone: allaccess</td>
<td>defzone: noaccess</td>
<td>Clean merge — noaccess takes precedence and defzone configuration from <strong>Switch B</strong> propagates to fabric. defzone: noaccess</td>
</tr>
<tr>
<td>Different default zone access mode settings.</td>
<td>defzone: noaccess</td>
<td>defzone: allaccess</td>
<td>Clean merge — noaccess takes precedence and defzone configuration from <strong>Switch A</strong> propagates to fabric. defzone: noaccess</td>
</tr>
</tbody>
</table>
Table 114  Zone merging scenarios (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Switch A</th>
<th>Switch B</th>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same default zone access mode settings.</td>
<td>defzone: allaccess</td>
<td>defzone: allaccess</td>
<td>Clean merge — defzone configuration is allaccess in the fabric.</td>
</tr>
<tr>
<td>Same default zone access mode settings.</td>
<td>defzone: noaccess</td>
<td>defzone: noaccess</td>
<td>Clean merge — defzone configuration is noaccess in the fabric.</td>
</tr>
<tr>
<td>Effective zone configuration.</td>
<td>No effective</td>
<td>effective: cfg2</td>
<td>Clean merge — effective zone configuration from Switch B propagates to fabric.</td>
</tr>
<tr>
<td>Effective zone configuration.</td>
<td>No effective</td>
<td>effective: cfg2</td>
<td>Fabric segments because Switch A has a hidden zone configuration (no access)</td>
</tr>
<tr>
<td></td>
<td>configuration.</td>
<td></td>
<td>activated and Switch B has an explicit zone configuration activated.</td>
</tr>
<tr>
<td></td>
<td>defzone = allaccess</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>defzone = noaccess</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Index

A
AAA service requests 67
aaaConfig command 69, 77, 79, 80
access
  browser support 89
  changing account parameters 61
  control 97
  CP blade 72
  creating accounts 60
  deleting accounts 60
  IP address changes 24
  log in fails 24
  NTP 32
  other devices 45
  other switches 45
  password, changing 26
  recovering accounts 62
  remote access policies 74
  secure, HTTPS 89
  secure, SSL 89
  SNMP ACL 85
access methods
  configuration, Fabric Manager 23
  configuration, Web Tools 23
accessControl 97
accessing switches and fabrics 88
account ID 24
account lockout policy 66
  duration 66
  threshold 66
accounts
  changing parameters 61
  creating 60
  deleting 60
  displaying information 59
  domain defaults 26
  managing passwords 62
  password rules 62
  recovering 62
  user-defined 59
activating
  a switch certificate 92
  Admin Domains 155
  certificates 92
  POD 40
  policy 108
  policy changes 108
  ports on demand 39
AD0 146
AD255 146
adding
  a new switch or fabric to a zone 410
  Admin Domain members 156
alias members 394
and removing FICON CUP licenses 273
custom filter-based monitors 349
devices, other 45
end-to-end monitors 346
filter-based monitors 349
members to a zone configuration 404
port mirror connection 324
RADIUS configuration 78
standard filter-based monitors 349
switches to a zone 410
zone members 397
ADList 71
Admin Domain configuration, displaying 159
Admin Domains
  activating and deactivating 155
  AD0 146
  AD255 146
  adding members 156
  assigning users to 154
  creating 153
  deleting 157
  firmware upgrade 151
  implementing 152
  interaction with Fabric OS features 160
  logging in to 148
  member types 148
  removing members 156
  renaming 156
  switch WWN 149
  switching context 160
  transaction model 152
  using 158
  validating members 158
advanced performance monitoring commands 344
agtCfgDefault 95
agtCfgSet 95
agtCfgShow 95
AIX procedure, PID 475
AL_PA 239
AL_PA monitoring 345
alias
  adding members 394
  creating 394
  deleting 395
  removing members 395
analyzing connection problems 304
assigning a static route 204
assigning users to Admin Domains 154
audience 19
Auth policy 109
authenticating users 55
authentication
  configuring 67
  local 80
auto-leveling, FR4-18i blade 173, 181

B
backbone fabric ID 218
backbone-to-edge routing 215, 218
backing up
   a configuration 135
basic
   card management 196
   PID procedure 472
basic connections 45
blocking listeners 88
boot password 80, 81, 83
boot PROM password 80
broadcast zones 391
Brocade Vendor-Specific Attribute 69
browser
   configuring 93
   troubleshooting certificates 94
browser and Java support 89
browser, configuration 93
browsers
   support 89

C
card management 196
certificates
   activating 92
   browser, configuring 93
   choosing 90
   corrupt 94
deleting 94
displaying 94
HTTPS 85
installing 92
invalid 94
not installed 94
obtaining 91
private key 90
public key 90
root 90
root, configuring 93
security 85
SSH 85
SSL 85, 89, 90
switch 90
troubleshooting 94
cfgActvShow command 257
changes to configuration data 465
changing
   an account password 64
   chassis name 193
   RADIUS configuration 79
   RADIUS servers 80
   switch names 33
to core PID format 469
CHAP
   account policies 74
   enabling 74
secPolicyShow 103
slotshow 217
supportsave 244
supportShow 244
userConfig 57
version 217

configuration
FICON environment switched point-to-point 262
FICON environment, cascaded 262
high-integrity fabric 265
save to a host 135
settings, FICON environment 264

configure 95, 98
configuring
access control 97
access methods, Fabric Manager 23
access methods, Web Tools 23
authentication 67
browser 93
browser, certificates 93
certificates 89
changing RADIUS servers 80
date and time 30
FibreAlliance MIB 95
FICON environment switches for 264
for interconnectivity 247
host 296
HTTPS access 89
IAS 73
IAS user 73
interfabric link 221
LINUX RADIUS server 72
NTP 32
private key 90
public key 90
RADIUS 74
RADIUS server 72
RADIUS, changing 79
root certificates 93
secure file copy 98
security features 85, 99
security levels 95
server database 283
SNMP 95
SNMP traps 95
SSL 89, 90
SSL protocol 89
switch 77, 264
switch for RADIUS 77
switch, FICON environment 264
switch, RADIUS client 73
switch, single 265
syslogd 296
telnet interface 87
Windows RADIUS client 73
zone, rules for 390

connecting
multiple EX_Ports to an edge fabric 216
other devices 45
other switches 45
connecting to devices 45
connecting to other switches 45
connecting to the command line interface 24
connection
restrictions 55
serial 24
telnet 24
conserving power 198
controlling access 280
controlling topology discovery 283
conventions
document 20
text symbols 20
core/edge topology and ISL trunking 374
correcting device login issues 313
correcting I2C bus errors 312
correcting link failures 317
correcting marginal links 319
correcting zoning setup issues 309
CP blade 35
access 72
CRC errors, displaying 345
creating
accounts 60
Admin Domains 153
alias 394
DCC policy 105
policy 105, 107
SCC policy 107
zone configurations 404
zones 396
CSR 91
customizing
switch names 33
customizing the chassis name 33
customizing the switch name 33

database, clearing in a FICON environment 263
date 30
date and time 30, 32
DCC
policy 105
deactivating Admin Domains 155
Default IP Policy Rules 119
default zone mode 399
defined AD configuration 152
defined zone configuration 386
defZone command 232
deleting
accounts 60
Admin Domains 157
alias 395
end-to-end monitors 348
filter-based monitors 351
policy 109
port mirror connection 324
RADIUS configuration 79
zone configurations 405
zones 398
deleting end-to-end monitors 348
deleting filter-based monitors 351
designing fabric for trunking 374
deskew 231
deskew values
  displaying 379
devices, connecting 45
devices, proxy 214
DH-CHAP 219
DHCHAP 220
DH-CHAP secret 220
dictionary.brocade 71
disabled zone configuration 387
disabling 44
  port 44
  RADIUS configuration 79
  switch 44
disabling and enabling a port 44
disabling and enabling a switch 33
disabling and enabling cards 197
displaying
  CRC error count 345
  node identification data, FICON environments 267
  RADIUS configuration 77
  registered listeners for link incidents, FICON
    environment 267
displaying and clearing the CRC error count 345
displaying and deleting certificates 94
displaying information 267
displaying mode register bit settings 271
displaying monitor counters 355
displaying the fmsmode setting 270
displaying trunking information 379
document
  conventions 20
  related documentation 20
domain
  default accounts 26
  default roles 26
Domain ID 33
domain ID, insistent 261
domain, phantom 215
downgrade
  and port mirroring 324
downloading configurations across a fabric 140
E
edge-to-edge routing 218
EF CM 251, 255
effective AD configuration 152
effective zone configuration 386
enabling
  CHAP 74
  port 44
  switch 44
enabling and disabling FICON management server
  mode 269
enabling and disabling ISL trunking 377
enabling and disabling local authentication 80
enabling and disabling the platform services 279
encryption 89
end-to-end monitoring 345
end-to-end monitors
  adding 346
  deleting 348
  restoring configuration 361
  saving configuration 361
  setting a mask 347
ensuring network security 86
evaluating the fabric 466
event
date and time 30
EX_Port 240, 250
Ex_Port 322
example
  chassisshow 46
  fabricshow 47
  nsallshow 47
  slotshow 47
exchange-based routing 203
F
fabric
  high integrity 262
fabric access 88
fabric connectivity 47
fabric considerations 374
Fabric Manager
  access methods 23
Fabric OS
  standard security features, configuring 85, 99
  supported protocols 85
Fabric Wide Consistency Policy 218
fabric, designing for trunking 374
fabricShow command 251
fabricshow command 47
fans, status of 293
Fastwrite 421, 424
FC Fastwrite 457
FC router 107
FC routing
  concepts 211
  supported platforms 211
FC routing types 215
FCAP 220
FC-FC Routing 107
FCIP 322
FCIP link 246
FCIP tunneling 417
fcrConfigure command 219
fcrProxyConfig command 228
fcrProxyDevShow command 255
fcrResourceShow command 239
fcrXlateConfig command 228
FCS policy
  modifying 101
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>fddCfg</td>
<td>218</td>
</tr>
<tr>
<td>fddCfg command</td>
<td>218</td>
</tr>
<tr>
<td>feature licenses</td>
<td>34</td>
</tr>
<tr>
<td>Fibre Channel NAT</td>
<td>215</td>
</tr>
<tr>
<td>Fibre Channel over IP</td>
<td>219, 417</td>
</tr>
<tr>
<td>Fibre Channel routing</td>
<td>211</td>
</tr>
<tr>
<td>FICON</td>
<td>323</td>
</tr>
<tr>
<td>FICON environment</td>
<td></td>
</tr>
<tr>
<td>cascaded configuration</td>
<td>262</td>
</tr>
<tr>
<td>configuration settings</td>
<td>264</td>
</tr>
<tr>
<td>disabling IDID mode</td>
<td>263</td>
</tr>
<tr>
<td>displaying link incidents</td>
<td>263</td>
</tr>
<tr>
<td>registered listeners for link incidents</td>
<td>267</td>
</tr>
<tr>
<td>enabling IDID mode</td>
<td>263</td>
</tr>
<tr>
<td>high integrity fabric</td>
<td>262</td>
</tr>
<tr>
<td>identifying port swapping nodes</td>
<td>268</td>
</tr>
<tr>
<td>monitoring FRU failures</td>
<td>267</td>
</tr>
<tr>
<td>node identification data, displaying</td>
<td>267</td>
</tr>
<tr>
<td>switched point-to-point configuration switches, configuring</td>
<td>262</td>
</tr>
<tr>
<td>FICON-MIB</td>
<td>95</td>
</tr>
<tr>
<td>file copy, secure</td>
<td>98</td>
</tr>
<tr>
<td>filter-based monitors</td>
<td>349</td>
</tr>
<tr>
<td>adding</td>
<td>349</td>
</tr>
<tr>
<td>deleting</td>
<td>351</td>
</tr>
<tr>
<td>restoring configuration</td>
<td>361</td>
</tr>
<tr>
<td>saving configuration</td>
<td>361</td>
</tr>
<tr>
<td>FIPS</td>
<td>177</td>
</tr>
<tr>
<td>firmware download</td>
<td>166</td>
</tr>
<tr>
<td>FirmwareDownload</td>
<td>324</td>
</tr>
<tr>
<td>fosConfig command</td>
<td>219</td>
</tr>
<tr>
<td>frame transfer with remote switch</td>
<td>499</td>
</tr>
<tr>
<td>FreeRADIUS</td>
<td>72</td>
</tr>
<tr>
<td>fru failures</td>
<td>267</td>
</tr>
<tr>
<td>fru failures, monitoring in FICON environments</td>
<td>263, 267</td>
</tr>
<tr>
<td>FTP</td>
<td>165</td>
</tr>
<tr>
<td>G</td>
<td></td>
</tr>
<tr>
<td>gateway</td>
<td>499</td>
</tr>
<tr>
<td>gateway, remote switch</td>
<td>499</td>
</tr>
<tr>
<td>gathering information for technical support</td>
<td>302</td>
</tr>
<tr>
<td>generating a public/private key</td>
<td>90</td>
</tr>
<tr>
<td>generating and storing a csr</td>
<td>91</td>
</tr>
<tr>
<td>H</td>
<td></td>
</tr>
<tr>
<td>HA failover</td>
<td>64, 72</td>
</tr>
<tr>
<td>hard zoning</td>
<td>387</td>
</tr>
<tr>
<td>hardware-enforced zoning</td>
<td>387</td>
</tr>
<tr>
<td>hashow command</td>
<td>47</td>
</tr>
<tr>
<td>help, obtaining</td>
<td>21, 22</td>
</tr>
<tr>
<td>high availability (HA)</td>
<td>46</td>
</tr>
<tr>
<td>high integrity fabric</td>
<td>262</td>
</tr>
<tr>
<td>HomeAD</td>
<td>71</td>
</tr>
<tr>
<td>host</td>
<td></td>
</tr>
<tr>
<td>configuring</td>
<td>296</td>
</tr>
<tr>
<td>host reboots</td>
<td>464</td>
</tr>
<tr>
<td>host-based zoning</td>
<td>384</td>
</tr>
<tr>
<td>HP</td>
<td></td>
</tr>
<tr>
<td>storage web site</td>
<td>22</td>
</tr>
<tr>
<td>Subscriber’s choice web site</td>
<td>22</td>
</tr>
<tr>
<td>technical support</td>
<td>21</td>
</tr>
<tr>
<td>HP/UX procedure</td>
<td>473</td>
</tr>
<tr>
<td>HTTP</td>
<td>92</td>
</tr>
<tr>
<td>HTTPS</td>
<td>89, 92, 94</td>
</tr>
<tr>
<td>certificates, security</td>
<td>85</td>
</tr>
<tr>
<td>hybrid update</td>
<td>469</td>
</tr>
<tr>
<td>I</td>
<td></td>
</tr>
<tr>
<td>IAS</td>
<td></td>
</tr>
<tr>
<td>configuring users</td>
<td>73</td>
</tr>
<tr>
<td>remote access policies</td>
<td>74</td>
</tr>
<tr>
<td>IAS (Internet Authentication Service), configuring</td>
<td>73</td>
</tr>
<tr>
<td>ID, account</td>
<td>24</td>
</tr>
<tr>
<td>identifying</td>
<td></td>
</tr>
<tr>
<td>ports from the tag field</td>
<td>274</td>
</tr>
<tr>
<td>identifying media-related issues</td>
<td>315</td>
</tr>
<tr>
<td>Identifying ports</td>
<td></td>
</tr>
<tr>
<td>by slot and port number</td>
<td>194</td>
</tr>
<tr>
<td>identifying ports</td>
<td></td>
</tr>
<tr>
<td>by port area ID</td>
<td>194</td>
</tr>
<tr>
<td>IDID</td>
<td>261</td>
</tr>
<tr>
<td>IDID mode</td>
<td></td>
</tr>
<tr>
<td>enabling and disabling in a FICON environment</td>
<td>266</td>
</tr>
<tr>
<td>IFL</td>
<td>211, 214, 216, 221</td>
</tr>
<tr>
<td>impact of changing the fabric PID format</td>
<td>464</td>
</tr>
<tr>
<td>implementing Admin Domains</td>
<td>152</td>
</tr>
<tr>
<td>inaccurate information in the system message log</td>
<td>320</td>
</tr>
<tr>
<td>initializing trunking on ports</td>
<td>375</td>
</tr>
<tr>
<td>insistent domain ID</td>
<td>261</td>
</tr>
<tr>
<td>installing</td>
<td></td>
</tr>
<tr>
<td>certificates</td>
<td>92</td>
</tr>
<tr>
<td>installing a root certificate to the Java plug-in</td>
<td>93</td>
</tr>
<tr>
<td>installing a switch certificate</td>
<td>92</td>
</tr>
<tr>
<td>interfabric link</td>
<td></td>
</tr>
<tr>
<td>configuring</td>
<td>221</td>
</tr>
<tr>
<td>interfabric link, see ISL</td>
<td></td>
</tr>
<tr>
<td>intermix mode</td>
<td>261</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>89</td>
</tr>
<tr>
<td>interopMode command</td>
<td>218</td>
</tr>
<tr>
<td>interswitch link</td>
<td>45</td>
</tr>
<tr>
<td>IP</td>
<td></td>
</tr>
<tr>
<td>switch address</td>
<td>33</td>
</tr>
<tr>
<td>IP security</td>
<td>420</td>
</tr>
<tr>
<td>ipAddrSet</td>
<td>27, 42</td>
</tr>
<tr>
<td>IPCOMP</td>
<td>420</td>
</tr>
<tr>
<td>IP-NAT</td>
<td>216</td>
</tr>
<tr>
<td>IPSec</td>
<td>420</td>
</tr>
<tr>
<td>changeable parameters</td>
<td>428</td>
</tr>
<tr>
<td>fixed parameters</td>
<td>428</td>
</tr>
<tr>
<td>ISL</td>
<td>45</td>
</tr>
<tr>
<td>maximums</td>
<td>45</td>
</tr>
<tr>
<td>J</td>
<td></td>
</tr>
<tr>
<td>Java support, SSL</td>
<td>89</td>
</tr>
<tr>
<td>Java version</td>
<td>89</td>
</tr>
</tbody>
</table>
K
  key
    transaction, for licensed features 34
  keys
    purchasing 39

L
  legacy FCR switches 241
  license ID 34
  license key
    activating 35
  licenseAdd command 35
  licensed features 34
  licenseShow 34
  licenseRemove command 36
  licenses
    license ID 34
    overview 34
    purchasing keys 39
    remove feature 36
    transaction key 34
  link incidents
    displaying in a FICON environment 263, 267
    linking through a gateway 45
  Linux, configuring RADIUS on 72
  listing link characteristics 381
  local account
    disabling 61
    enabling 61
  local authentication
    overview 80
  local clock 32
  LOCL 32
  log in
    fails 24
  logging
    timestamp 30
  login
    changing password 62
      switch 24
      with Admin Domains 148
  login sessions, maximum allowed 55
  LSAN 231
  LSAN zoning 255
  lsanShow command 257
  LUN sharing 246
  LWL
    ISL Trunking support for 373

M
  M_Port 322
  maintaining zones 396
  making basic connections 45
  managing
    accounts 62
    zoning configurations in a fabric 407
  managing shared secrets 114
  mask for end-to-end monitors
    setting 347
  matching fabric parameters 216
  McDATA 251
  members
    policy 100
    policy, adding 108
    policy, removing 109
  merging zones 400
  MIB 95, 96
  mibCapability 97
  modifying
    zoning configurations 404
  modifying the FCS policy 101
  monitoring
    AL_PAs 345
    monitoring end-to-end performance 345
    monitoring filter-based performance 349
    monitoring ISL performance 351
    monitoring resources 237
    monitoring traffic 375
    monitoring trunks 355
    monitors
      clearing counters 359
    most common problem areas 301
    Mozilla 89

N
  NAT 216
  network address translation, see NAT
  network security 86
  node identification data 267
  normal operation, FC routing 244
  NR_Port 239
  nsAllShow command 251, 256
  nsAllShow command 47
  nsCamShow command 256
  nsshow command 47
  NTP
    access 32

O
  obtaining and unzipping firmware 167
  obtaining certificates 91
  obtaining slot information 201
  offline update 469
  online update 468

P
  passwd command 62
  passwdCfg command 64
  password 24
    boot prom 80
    changing 62
    changing defaults 26
    default 26
    limits 26
  PROM 80, 81, 83
  recovery 83
recovery string 81
rules 62
set PROM 81, 82
password expiration policy 65
password management information 495
password migration during firmware changes 497
password policies 63
password prompting behaviors 496
password recovery options 497
password strength policy 64
passwords
  recovering forgotten passwords 84
perfaddeemonitor command 346
perfaddIPmonitor command 349
perfaddusermonitor command 350
perfcfgrestore command 361
perfcfgsave command 361
perfdeleemonitor command 348
perfdelfiltermonitor command 351
performance monitoring commands 344
performing PID format changes 470
perfsetportemask command 347
perfshowalpacrc command 345
permissions and roles 57
persistently enabling/disabling ports 272
phantom domains 213, 216
physical fabric administrator 147
PID
  AIX procedure 475
PKI 89
planning the update procedure 468
platforms, FC routing supported 211
POD
  activating 40
  enabling ports 44
policy
  account lockout 66
  activating 108
  adding members 108
  changes, activating 108
  changes, saving 108
  creating 105, 107
  creating, DCC 105
  creating, SCC 107
  DCC 105
  deleting 109
  members, adding 108
  members, identifying 100
  members, removing 109
  password expiration 65
  password strength 64
  SCC 107
port 44
  enabling 44
  port and switch naming standards 273
port mirroring 322
port swapping nodes, identifying in FICON environments 268
port-based routing 203
portDisable 115
portEnable 115
portLog command 255
ports
  activating POD 40
  identifying by port area ID 194
  identifying by slot and port number 194
  status of 289
ports, swapping 268
powering off a card 197
powering port cards on and off 196
preparing a switch 265
private key 90
PROM
  password 80, 81, 83
  recovery string 81
  set password 81
  set password 81, 82
protocols
  secure 85
proxy
  devices 214
  proxy PID 213, 228
public key 90
public key infrastructure encryption 89
R
rack stability, warning 21
RADIUS 74, 77, 78, 79, 80
RADIUS client
  Windows configuration 73
RADIUS clients
  switch configuration 73
RADIUS server 70
  configuration 72
  configuring 72
  LINUX configuration 72
RADIUS service
  Windows configuration 73
RBAC 56
reboot 239
recognizing buffer underallocation 382
recognizing MQ-WRITE errors 312
recognizing the port initialization and FCP auto discovery process 322
recording configuration information 276
recovering
  accounts 62
  recovering forgotten passwords 84
  recovery password 83
recovery string 81
recovery string, boot PROM password 80
registered listeners 267
related documentation 20
remote access policies 74
remote switch 499
remove feature 36
removing
  Admin Domain members 156
  alias members 395
end-to-end monitors 348
filter-based monitors 351
licensed feature 36
members from a zone configuration 405
zone members 398
renaming Admin Domains 156
resolving zone conflicts 412
restoring a configuration 137
restoring a segmented fabric 307
restoring configurations in a FICON environment 140
restoring monitor configuration 361
restoring the system configuration settings 137
Role-Based Action Control. See RBAC.
roles
  domain defaults 26
routing
  assigning a static route 204
routing policies 203
RSCN 33
rules
  configuring zones, for 390
password 62
S
SAN Pilot 251, 255
saved zone configuration 386
saving
  policy 108
  policy changes 108
saving and restoring monitor configurations 361
saving monitor configuration 361
scalability 246
SCC
  policy 107
SCC list 220
secCertUtil 94
seccertutil 90, 91, 92
Secure Fabric OS 220
secure file copy
  configuring 98
secure shell (ssh) 86
secure socket layer protocol 89
secure sockets layer 89
security 86
  activating certificates 92
  and tunneling 420
  Brocade MIB 95
  browsers 89
  certificates 85
certificates, deleting 94
  certificates, displaying 94
  configuring standard features 85, 99
  enabling CHAP 74
  encryption 89
  FibreAlliance MIB 95
  file copy 98
  HTTPS, certificate 85
  IAS remote access policies 74
  obtaining certificates 91
  secure protocols, supported 85
  setting levels 95
  SNMP traps 95
  SSH, certificate 85
  SSL, certificate 85
security and zoning 412
selecting a PID format 465
Selecting Authentication Protocols 113
sequential devices 421, 424
serial connection 24, 25
server database
  configuring 283
sessions, maximum allowed 55
setting
  time zone 31
setting a mask for end-to-end monitors 347
setting a unique domain id 266
setting mask for end-to-end monitors 347
setting mode register bits 272
setting port speeds 378
setting the boot prom password 80, 81
setting the date and time 30
setting the default account passwords 30
setting the IP address 28
setting the security level 95
setting the switch date and time 30
Setting time zones 30
setting up automatic trace dump transfers 298
settings
  changing passwords 26
  CHAP local security 74
date and time 30
  PROM password 81, 82
  security level 95
setup summary 269
shared secrets
  managing 114
SID 323
SLAP 220
slotShow command 217
slotshow command 47
SNMP 95
  ACL 85
  agent 85
  and password change 62
  configuring 95
SNMP attributes 95
snmpConfig 95, 96
snmpconfig 96, 97
snmpMibCapSet 95
SNMPv1 95, 97
SNMPv3 95, 96
specifying frame order delivery 204
specifying the routing policy 203
speeds
  ISL 45
SSH
  certificates 85
SSL 89, 90, 92, 94
certificates, security 85
SSL protocol
  configuring 89
standard filter-based monitors 349
standard trunking criteria 374
standby
  CP blade 72
static PID mapping errors 464
static route 204
storage-based zoning 384
Subscriber's choice, HP 22
summary of PID formats 463
summary of SSL procedures 90
support
  FC router 107
  Java version 89
  SNMPv3 and v1 95
supported
  optional licensed features 482
Supported Services 118
supportSave command 244
supportsave command 298
supportShow command 244
swapping port area IDs 476
swapping ports 268
SW-EXTTRAP 95
switch
  access methods, Fabric Manager 23
  access methods, Web Tools 23
  certificates, installing 92
  configuring 77, 264
  configuring single 265
  connecting 45
  deleting RADIUS configuration 79
  disabling 44
  disabling port 44
  displaying RADIUS configuration 77
  enabling 44
  FICON environment, configuring 264
  identifying 33
  IP 33
  name
    customizing 33
    name limitations 33
  RADIUS client 73
  RADIUS configuration 77
  RADIUS configuration, adding 78
  RADIUS configuration, disabling 79
  system status 287
  user-defined accounts 59
switch access 88
Switch Connection Controls list 220
switch names 33
switch WWN in Admin Domains 149
switchShow command 250
swtichshow command 46
SWL, ISL Trunking support for 373
symbols in text 20
synchronize
date and time 32
syslogd
  configuring 296
system-defined Admin Domains 145
systemGroup 98
T
tag field, interpreting 274
Tape pipelining 421, 424
tape write acceleration 421, 424
TCP/IP 420
technical support, HP 21
telnet
  configuring 87
telnet connection 24
temperature, status of 293
text symbols 20
time 30
time and date 30
time zones 30, 32
tracking and controlling switch changes 48
traffic patterns
  planning for 375
transaction key 34
traps
  MIB 95
  SNMP 95
troubleshooting 274
certificates 94
corrupt certificate 94
invalid certificate 94
port mirroring 322
troubleshooting certificates 94
troubleshooting the migration 184
troubleshooting trunking problems 381
trunking
  displaying information 379
  trunking over extended fabrics 380
tsclockserver 31, 32
tsTimeZone 30, 31
tunneling
  and security 420
U
unsupported features 483
upgrading switches 169
USB 176
USB device 176
user databases 63
user, local
  disabling 61
  enabling 61
userConfig command 57, 60, 61
user-defined
  accounts 59
user-defined Admin Domains 145
user-defined filter-based monitors 350
users, authenticating 55
using
certificates 89
using dynamic load sharing 205
using FICON CUP 268
using legacy commands for SNMPv1 98
using the snmpconfig command 96
using zoning to administer security 412

V
validating Admin Domain members 158
VC_RDY 369
VE_Port 322
verification check 217
verify
device connectivity 45
high availability (HA) 46
version command 217
VEX_Port 417
viewing
alias 396
fan status 293
port status 289
power supply status 293
temperature status 293
zones 398
viewing and saving diagnostic information 298
viewing equipment status 293
viewing port information 289
viewing power-on self test 285
viewing routing information along a path 208
viewing routing path information 206
viewing switch status 287
viewing the port log 294
viewing the system message log 294
viewing zone database configurations 407
VSA 69

W
warning
rack stability 21
web sites
HP storage 22
HP Subscriber’s choice 22
Web Tools
access methods 23
Windows RADIUS, configuring 73
working with domain IDs 33
WWN 33, 35

X
xlate domains 213

Z
zone
adding members 397
adding switches 410
administering security 412
aliases 386
aliases, creating and managing 394
configurations 386
configurations, creating and maintaining 404
configuring rules 390
creating 396
creating a configuration 404
database size 400
default zone mode 399
defined zone configuration 386
deleting 398
deleting a configuration 405
disabled zone configuration 387
effective zone configuration 386
enforcement 387
hard zoning 387
hardware-enforced zoning 387
host-based 384
LUN masking 384
maintaining 396
merging 400
name server-based 384
objects 385
optimizing resources 383
removing members 398
removing members from a configuration 405
resolving conflicts 412
saved zone configuration 386
schemes 386
soft-zoning 384
splitting a fabric 412
storage-based 384
troubleshooting 412
types 384
viewing 398
viewing configurations 407
zone configuration
adding members 404
zone name restrictions 486
zone, broadcast 391
zoning
and PDCM considerations 273
LSAN 255
zoning restrictions 486