CONTENTS

ABOUT THIS GUIDE
Conventions 25
Documentation 26
Documentation Comments 27

NEW FEATURES SUMMARY
Virtual Controller Clustering Configuration 30
   set cluster mode 30
   set cluster preempt 30
AP 3950 PoE Configuration 31
   set ap power-mode 31
802.11n Configuration 31
   set service-profile 11n 32
   set service-profile transmit-rates 32
   set radio-profile 11n 33
External Captive Portal Support 33
Simultaneous Login Support 34
Dynamic RADIUS Extensions 34
   set radius dac 34
   set radius das-port 34
   clear radius das-port 35
   set authorization dynamic 35
   termination-action Attribute 35
MAC User Range Authentication 36
   set authentication mac-prefix 36
MAC Authentication Request Format 37
User Attribute Enhancements 37
Enhancements to Location Policy Configuration 38
RADIUS Ping Utility 39
   radping 39
Unique AP Number Support 40
Bandwidth Management 40
  set qos profile 40
  set radio-profile weighted-fair-queuing 41
  set service-profile max-bw 42
  clear qos-profile 42
RF Scanning Enhancements 43
  set radio-profile rf-scanning mode 43
  set radio-profile rf-scanning channel-scope 44
RF Detection Configuration 44
  Deprecated Commands 44
  Replaced Commands 45
  set rfdetect ssid-list 45
  set rfdetect classification ad-hoc 45
  set rfdetect classification default 46
  set rfdetect classification seen-in-network 46
  set rfdetect classification ssid-masquerade 47
  display rfdetect classification 47
display aaa Command Replacements 48
  display radius 48
  display user 49
  display mac-user 51
  display usergroup 52
  display mac-usergroup 53
display ap config Enhancements 54
  display ap config 54
  display ap config verbose 54
  display ap config radio 55
display load Enhancements 55
  display load memory 56
  display load cpu 57
  display load cpu history 58
display radio-profile Enhancements 58
  display radio-profile 59
display sessions network ap Enhancements 60
  display sessions network ap 60
  display sessions network ap radio 60
clear sessions network Enhancements 61
1 Using the Command-Line Interface

Overview 75

CLI Conventions 76

Command Prompts 76

Syntax Notation 76

Text Entry Conventions and Allowed Characters 77

MAC Address Notation 77

IP Address and Mask Notation 78

User Globs, MAC Address Globs, and VLAN Globs 78

Port Lists 80

Virtual LAN Identification 81

Command-Line Editing 81

Keyboard Shortcuts 81

History Buffer 82

Tabs 82

Single-Asterisk (*) Wildcard Character 82

Double-Asterisk (**) Wildcard Characters 82

Using CLI Help 83

Understanding Command Descriptions 84

2 Access Commands

Commands by Usage 85

disable 85

enable 86

quit 86

set enablepass 87
3 **SYSTEM SERVICE COMMANDS**

Commands by Usage 89
- clear banner motd 90
- clear history 91
- clear prompt 91
- clear system 92
- display banner motd 93
- display base-information 93
- display license 94
- display load 95
- display system 95
- help 98
- history 99
- quickstart 100
- set auto-config 100
- set banner acknowledge 102
- set banner motd 104
- set confirm 105
- set length 105
- set license 106
- set prompt 107
- set system contact 108
- set system countrycode 109
- set system idle-timeout 113
- set system ip-address 114
- set system location 115
- set system name 116

4 **PORT COMMANDS**

Commands by Usage 117
- clear ap 118
- clear port counters 119
- clear port-group 119
- clear port media-type 120
- clear port name 120
- clear port mirror 121
- clear port preference 121
clear port type 122
display port counters 123
display port-group 124
display port mirror 125
display port poe 126
display port status 127
display port media-type 129
monitor port counters 130
reset port 135
set ap 135
set port 137
set port-group 138
set port media-type 139
set port mirror 140
set port name 141
set port negotiation 141
set port poe 142
set port speed 143
set port trap 144
set port type ap 145
set port type wired-auth 148

5 **VLAN Commands**

Commands by usage 151
clear fdb 152
clear security L2-restrict 153
clear security L2-restrict counters 154
clear vlan 155
clear vlan-profile 156
display fdb 157
display fdb agingtime 159
display fdb count 160
display roaming station 161
display roaming vlan 163
display security L2-restrict 164
display tunnel 165
display vlan config 166
display vlan-profile 168
set fdb 169
set fdb agingtime 170
set security L2-restrict 171
set vlan name 172
set vlan port 173
set vlan tunnel-affinity 174
set vlan profile 175

6 QUALITY OF SERVICE COMMANDS
Commands by Usage 177
clear qos 177
set qos cos-to-dscp-map 179
set qos dscp-to-cos-map 180
display qos 181
display qos dscp-table 182

7 IP SERVICES COMMANDS
Commands by Usage 183
clear interface 185
clear ip alias 186
clear ip dns domain 187
clear ip dns server 187
clear ip route 188
clear ip telnet 189
clear ntp server 189
clear ntp update-interval 190
clear snmp community 191
clear snmp notify profile 191
clear snmp notify target 192
clear snmp usm 192
clear summertime 193
clear system ip-address 194
clear timezone 194
display arp 195
display dhcp-client 196
display dhcp-server 198
display interface 200
display ip alias 201
display ip dns 202
display ip https 203
display ip route 204
display ip telnet 206
display ntp 207
display snmp community 209
display snmp counters 210
display snmp notify profile 210
display snmp notify target 210
display snmp status 211
display snmp usm 212
display summertime 212
display timedate 213
display timezone 213
ping 214
set arp 216
set arp agingtime 217
set interface 218
set interface dhcp-client 219
set interface dhcp-server 220
set interface status 221
set ip alias 222
set ip dns 223
set ip dns domain 223
set ip dns server 224
set ip https server 225
set ip route 226
set ip snmp server 228
set ip ssh 228
set ip ssh server 229
set ip telnet 229
set ip telnet server 230
set ntp 231
set ntp server 232
set ntp update-interval 233
set snmp community 233
set snmp notify profile 235
set snmp notify target 240
SNMPv3 with Informs 240
SNMPv3 with Traps 241
SNMPv2c with Informs 242
SNMPv2c with Traps 243
SNMPv1 with Traps 243
set snmp protocol 245
set snmp security 246
set snmp usm 247
set summertime 250
set system ip-address 251
set timedate 252
set timezone 253
telnet 254
traceroute 255

8 AAA COMMANDS
Commands by Usage 259
clear accounting 261
clear authentication admin 262
clear authentication console 263
clear authentication dot1x 264
clear authentication mac 265
clear authentication proxy 266
clear authentication web 266
clear location policy 267
clear mac-user 268
clear mac-user attr 269
clear mac-user group 269
clear mac-usergroup 270
clear mac-usergroup attr 271
clear mobility-profile 272
clear user 272
clear user attr 273
clear user group 274
clear user lockout 274
clear usergroup 275
clear usergroup attr 276
display aaa 277
display accounting statistics 280
display location policy 282
display mobility-profile 283
set accounting {admin | console} 283
set accounting {dot1x | mac | web | last-resort} 285
set authentication admin 287
set authentication console 289
set authentication dot1x 291
set authentication mac 295
set authentication max-attempts 297
set authentication max-attempts 298
set authentication minimum-password-length 299
set authentication password-restrict 300
set authentication proxy 301
set authentication web 302
set location policy 304
set mac-user 308
set mac-user attr 309
set mac-usergroup attr 315
set mobility-profile 317
set mobility-profile mode 319
set user 319
set user attr 321
set user expire-password-in 322
set user group 323
set usergroup 323
set usergroup expire-password-in 325
set web-portal 326

9 MOBILITY DOMAIN COMMANDS

Commands by Usage 327
clear mobility-domain 328
clear mobility-domain member 328
display mobility-domain 329
display mobility-domain config 330
display mobility-domain status 331
set mobility-domain member 332
set mobility-domain mode member secondary seed-ip 333
set mobility-domain mode member seed-ip 334
set mobility-domain mode secondary-seed domain-name 335
set mobility-domain mode seed domain-name 336
set domain security 337

10 NETWORK DOMAIN COMMANDS
Network Domain Commands by Usage 339
clear network-domain 340
clear network-domain mode 341
clear network-domain peer 342
clear network-domain seed-ip 343
display network-domain 344
set network-domain mode member seed-ip 346
set network-domain peer 347
set network-domain mode seed domain-name 348

11 MANAGED ACCESS POINT COMMANDS
MAP Access Point Commands by Usage 349
clear ap local-switching vlan-profile 355
clear ap radio 356
clear ap boot-configuration 358
clear ap radio load-balancing group 359
clear radio-profile 360
clear service-profile 361
display ap arp 362
display ap config 364
display ap counters 367
display ap fdb 373
display ap qos-stats 374
display ap etherstats 375
display ap group 377
display ap mesh-links 377
display ap status 379
display ap vlan  385
display auto-tune attributes  386
display auto-tune neighbors  388
display ap boot-configuration  390
display ap connection  391
display ap global  393
display ap unconfigured  395
display load-balancing group  396
display radio-profile  398
display service-profile  401
reset ap  410
set ap auto  410
set ap auto persistent  412
set ap auto radiotype  413
set ap auto mode  414
set ap bias  415
set ap blink  416
set ap boot-configuration ip  417
set ap boot-configuration mesh mode  418
set ap boot-configuration mesh psk-phrase  419
set ap boot-configuration mesh psk-raw  420
set ap boot-configuration mesh ssid  421
set ap boot-configuration switch  422
set ap boot-configuration vlan  423
set ap contact  424
set ap fingerprint  424
set ap force-image-download  426
set ap group  427
set ap location  427
set ap local-switching mode  427
set ap local-switching vlan-profile  428
set ap name  429
set ap radio antenna-location  430
set ap radio antennatype  431
set ap radio auto-tune max-power  432
set ap radio auto-tune max-retransmissions  433
set ap radio channel 435
set ap radio link-calibration 436
set ap radio load balancing 437
set ap radio load balancing group 438
set ap radio mode 439
set ap radio radio-profile 440
set ap radio tx-power 441
set ap security 443
set ap upgrade-firmware 444
set band-preference 445
set load-balancing mode 446
set load-balancing strictness 447
set radio-profile 11g-only 448
set radio-profile active-scan 448
set radio-profile auto-tune 11a-channel-range 449
set radio-profile auto-tune channel-config 450
set radio-profile auto-tune channel-holddown 451
set radio-profile auto-tune channel-interval 452
set radio-profile auto-tune channel-lockdown 453
set radio-profile auto-tune power-config 454
set radio-profile auto-tune power-interval 455
set radio-profile auto-tune power-lockdown 456
set radio-profile auto-tune power-ramp-interval 457
set radio-profile beacon-interval 457
set radio-profile countermeasures 458
set radio-profile dtim-interval 460
set radio-profile frag-threshold 461
set radio-profile long-retry 462
set radio-profile max-rx-lifetime 462
set radio-profile max-tx-lifetime 463
set radio-profile mode 464
set radio-profile preamble-length 467
set radio-profile qos-mode 468
set radio-profile rfid-mode 469
set radio-profile rate-enforcement 469
set radio-profile rts-threshold 471
set radio-profile service-profile 472
set radio-profile short-retry 478
set service-profile tkip-mc-time 514
set service-profile static-cos 515
set service-profile transmit-rates 516
set service-profile use-client-dscp 518
set service-profile user-idle-timeout 519
set service-profile web-portal-acl 520
set service-profile web-portal-form 521
set service-profile web-portal-logout logout-url 523
set service-profile web-portal-logout mode 524
set service-profile web-portal-session-timeout 525
set service-profile wep active-multicast-index 526
set service-profile wep active-unicast-index 527
set service-profile wep key-index 528
set service-profile wpa-ie 529

12 **STP COMMANDS**

STP Commands by Usage 531

clear spantree portcost 532
clear spantree portpri 533
clear spantree portvlancost 533
clear spantree portvlanpri 534
clear spantree statistics 535
display spantree 536
display spantree backbonefast 539
display spantree blockedports 540
display spantree portfast 541
display spantree portvlancost 542
display spantree statistics 542
display spantree uplinkfast 548
set spantree 549
set spantree backbonefast 550
set spantree fwddelay 551
set spantree hello 551
set spantree maxage 552
set spantree portcost 553
set spantree portfast 554
set spantree portpri 555
set spantree portv lancost 556
set spantree portvlanpri 557
set spantree priority 558
set spantree uplinkfast 558

13 IGMP SNOOPING COMMANDS
Commands by usage 561
clear igmp statistics 562
display igmp 562
display igmp mrouter 566
display igmp querier 567
display igmp receiver-table 569
display igmp statistics 571
set igmp 573
set igmp lmqi 574
set igmp mrouter 575
set igmp mrsol 576
set igmp mrsol mrsi 576
set igmp oqi 577
set igmp proxy-report 578
set igmp qi 579
set igmp qri 580
set igmp querier 581
set igmp receiver 581
set igmp rv 582

14 SECURITY ACL COMMANDS
Security ACL Commands by Usage 585
clear security acl 586
clear security acl map 587
commit security acl 589
display security acl 590
display security acl editbuffer 591
display security acl hits 592
display security acl info 593
display security acl map 594
display security acl resource_usage 595
collapse security acl 599
set security acl 600
set security acl map 605
set security acl hit-sample-rate 607

15 CRYPTOGRAPHY COMMANDS
Commands by Usage 610
crypto ca-certificate 610
crypto certificate 612
crypto generate key 613
crypto generate request 614
crypto generate self-signed 616
crypto otp 618
crypto pkcs12 620
display crypto ca-certificate 621
display crypto certificate 622
display crypto key domain 624
display crypto key ssh 624

16 RADIUS AND SERVER GROUP COMMANDS
Commands by Usage 625
clear radius 626
clear radius client system-ip 627
clear radius proxy client 628
clear radius proxy port 628
clear radius server 629
clear server group 629
set radius 630
set radius client system-ip 632
set radius proxy client 633
set radius proxy port 634
set radius server 635
set server group 637
set server group load-balance 638
17  **802.1X MANAGEMENT COMMANDS**

Commands by Usage  641

- clear dot1x bonded-period  642
- clear dot1x max-req  643
- clear dot1x port-control  643
- clear dot1x quiet-period  644
- clear dot1x reauth-max  645
- clear dot1x reauth-period  645
- clear dot1x timeout auth-server  646
- clear dot1x timeout supplicant  646
- clear dot1x tx-period  647
- display dot1x  647
- set dot1x authcontrol  650
- set dot1x bonded-period  651
- set dot1x key-tx  652
- set dot1x max-req  653
- set dot1x port-control  654
- set dot1x quiet-period  655
- set dot1x reauth  655
- set dot1x reauth-max  656
- set dot1x reauth-period  657
- set dot1x timeout auth-server  657
- set dot1x timeout supplicant  658
- set dot1x tx-period  658
- set dot1x wep-rekey  659
- set dot1x wep-rekey-period  660

18  **SESSION MANAGEMENT COMMANDS**

Commands by Usage  661

- clear sessions  661
- clear sessions network  663
- display sessions  664
- display sessions mesh-ap  667
- display sessions network  668
19 RF DETECTION COMMANDS

Commands by Usage  677
clear rfdetect attack-list  678
clear rfdetect black-list  679
clear rfdetect ignore  679
clear rfdetect ssid-list  680
clear rfdetect vendor-list  681
rping  682
display rfdetect attack-list  683
display rfdetect black-list  684
display rfdetect clients  685
display rfdetect countermeasures  687
display rfdetect counters  688
display rfdetect data  690
display rfdetect ignore  692
display rfdetect mobility-domain  692
display rfdetect ssid-list  697
display rfdetect vendor-list  697
display rfdetect visible  698
set rfdetect active-scan  700
set rfdetect attack-list  701
set rfdetect black-list  702
set rf detect countermeasures  702
set rfdetect countermeasures mac  703
set rfdetect ignore  704
set rfdetect log  705
set rfdetect signature  706
set rfdetect signature key  707
set rfdetect ssid-list  707
set rfdetect vendor-list  708
test rflink  709

20 FILE MANAGEMENT COMMANDS

Commands by Usage  711
backup  712
clear boot backup-configuration  714
clear boot config  714
copy 715
delete 717
dir 718
install soda agent 721
display boot 722
display config 723
display version 725
load config 727
md5 729
mkdir 729
reset system 731
restore 732
rmdir 733
save config 733
set boot backup-configuration 734
set boot configuration-file 735
set boot partition 736
uninstall soda agent 736

21 TRACE COMMANDS
Commands by Usage 739
clear log trace 740
clear trace 740
display trace 741
save trace 742
set trace authentication 742
set trace authorization 743
set trace dot1x 744
set trace sm 745

22 SNOOP COMMANDS
Commands by Usage 747
clear snoop 748
clear snoop map 748
set snoop 749
set snoop map 752
set snoop mode 753
display snoop 754
display snoop info 754
display snoop map 755
display snoop stats 756

23 SYSTEM LOG COMMANDS
Commands by Usage 759
clear log 759
display log buffer 760
display log config 762
display log trace 763
set log 764
set log mark 767

24 BOOT PROMPT COMMANDS
Boot Prompt Commands by Usage 769
autoboot 770
boot 771
change 773
create 774
delete 775
dhcp 776
diag 777
dir 777
display 778
fver 780
help 781
ls 782
next 783
reset 784
test 785
version 786

A OBTAINING SUPPORT FOR YOUR 3COM PRODUCTS
Register Your Product to Gain Service Benefits 787
Solve Problems Online 787
ABOUT THIS GUIDE

This command reference explains Mobility System Software (MSS™) command line interface (CLI) that you enter on a 3Com WXR100 or WX1200 Wireless Switch or WX4400 or WX2200 Wireless LAN Controller to configure and manage the Mobility System™ wireless LAN (WLAN).

Read this reference if you are a network administrator responsible for managing WXR100, WX1200, WX4400, or WX2200 wireless switches and their Managed Access Points (MAPs) in a network.

If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the 3Com World Wide Web site:

http://www.3com.com/

Table 1 and Table 2 list conventions that are used throughout this guide.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Information note" /></td>
<td>Information note</td>
<td>Information that describes important features or instructions</td>
</tr>
<tr>
<td><img src="image" alt="Caution" /></td>
<td>Caution</td>
<td>Information that alerts you to potential loss of data or potential damage to an application, system, or device</td>
</tr>
</tbody>
</table>
This manual uses the following text and syntax conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monospace text</td>
<td>Sets off command syntax or sample commands and system responses.</td>
</tr>
<tr>
<td>Bold text</td>
<td>Highlights commands that you enter or items you select.</td>
</tr>
<tr>
<td>Italic text</td>
<td>Designates command variables that you replace with appropriate values, or highlights publication titles or words requiring special emphasis.</td>
</tr>
<tr>
<td>[ ] (square brackets)</td>
<td>Enclose optional parameters in command syntax.</td>
</tr>
<tr>
<td>{ } (curly brackets)</td>
<td>Enclose mandatory parameters in command syntax.</td>
</tr>
<tr>
<td></td>
<td>(vertical bar)</td>
</tr>
<tr>
<td>Keyboard key names</td>
<td>If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del</td>
</tr>
<tr>
<td>Words in italics</td>
<td>Italics are used to:</td>
</tr>
<tr>
<td></td>
<td>* Emphasize a point.</td>
</tr>
<tr>
<td></td>
<td>* Denote a new term at the place where it is defined in the text.</td>
</tr>
<tr>
<td></td>
<td>* Highlight an example string, such as a username or SSID.</td>
</tr>
</tbody>
</table>

### Documentation

The MSS documentation set includes the following documents.

- **Wireless Switch Manager (3WXM) Release Notes**
  These notes provide information about the 3WXM software release, including new features and bug fixes.

- **Wireless LAN Switch and Controller Release Notes**
  These notes provide information about the MSS software release, including new features and bug fixes.

- **Wireless LAN Switch and Controller Quick Start Guide**
  This guide provides instructions for performing basic setup of secure (802.1X) and guest (WebAAA™) access, for configuring a Mobility Domain for roaming, and for accessing a sample network plan in 3WXM for advanced configuration and management.
Wireless Switch Manager Reference Manual
This manual shows you how to plan, configure, deploy, and manage a Mobility System wireless LAN (WLAN) using the 3Com Wireless Switch Manager (3WXM).

Wireless Switch Manager User’s Guide
This manual shows you how to plan, configure, deploy, and manage the entire WLAN with the 3WXM tool suite. Read this guide to learn how to plan wireless services, how to configure and deploy 3Com equipment to provide those services, and how to optimize and manage your WLAN.

Wireless LAN Switch and Controller Hardware Installation Guide
This guide provides instructions and specifications for installing a WX wireless switch in a Mobility System WLAN.

Wireless LAN Switch and Controller Configuration Guide
This guide provides instructions for configuring and managing the system through the Mobility System Software (MSS) CLI.

Wireless LAN Switch and Controller Command Reference
This reference provides syntax information for all MSS commands supported on WX switches.

Documentation Comments
Your suggestions are very important to us. They will help make our documentation more useful to you. Please e-mail comments about this document to 3Com at:

pddtechpubs_comments@3com.com

Please include the following information when contacting us:

- Document title
- Document part number and revision (on the title page)
- Page number (if appropriate)

Example:

- Wireless LAN Switch and Controller Configuration Guide
- Part number 730-9502-0071, Revision B
- Page 25
Please note that we can only respond to comments and questions about 3Com product documentation at this e-mail address. Questions related to Technical Support or sales should be directed in the first instance to your network supplier.
NEW FEATURES SUMMARY

This summary describes new features and commands available in Version 7.0 of the Wireless LAN Mobility System that affect this guide. Each feature section includes:

- A brief description of the feature or command
- Basic configuration procedures, if applicable

It is important to note that new MSS 7.0 features and commands are **not** described within the individual chapters of this guide. They are only covered in this summary section.

This summary covers the following topics:

- Virtual Controller Clustering Configuration on page 30
- AP 3950 PoE Configuration on page 31
- External Captive Portal Support on page 33
- Simultaneous Login Support on page 34
- Dynamic RADIUS Extensions on page 34
- MAC User Range Authentication on page 36
- MAC Authentication Request Format on page 37
- User Attribute Enhancements on page 37
- Enhancements to Location Policy Configuration on page 38
- RADIUS Ping Utility on page 39
- Unique AP Number Support on page 40
- Bandwidth Management on page 40
- RF Scanning Enhancements on page 43
- RF Detection Configuration on page 44
- display aaa Command Replacements on page 48
Virtual Controller Clustering Configuration

New commands support configuration of virtual controller clustering on a mobility domain.

set cluster mode

Enable virtual controller cluster configuration on WXs in a mobility domain.

Syntax — set cluster mode {enable | disable} preempt {enable | disable}

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 7.0.

Usage — You must enable cluster mode on all WXs that are members of the cluster.

Examples — The following command enables cluster mode on a WX in a mobility domain:
WX# set cluster mode enable
success: change accepted

set cluster preempt

Use this command on the secondary seed of the cluster to allow the secondary seed to become active if the primary seed fails.
Syntax — `set cluster preempt {enable | disable}`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 7.0.

Usage — You can only use this command on the secondary seed of the mobility domain.

Examples — The following command enables preempt mode on a secondary seed:

```
WX# set cluster preempt enable
success:change accepted
```

**AP 3950 PoE Configuration**

A new command supports PoE configuration on the AP 3950.

```
set ap power-mode
```

Syntax — `set ap apnum power-mode {auto | high}`

- **auto** — Power is managed automatically by sensing the power level on the AP. If low power is detected, unused Ethernet is disabled and reduces the traffic on the 2.4 GHz radio. If high power is detected, then both radios operate at 3x3 (3 transmit chains and 3 receive chains).

- **high** — Both radios operate at the maximum power available, which requires either 802.3at PoE or both ports using 802.3af PoE.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 7.0.

**802.11n Configuration**

These commands support configuration of 802.11n frame aggregation, data rates, and channel width on the AP 3950.
set service-profile 11n

A new command to configure maximum MPDU and MSDU packet length, frame aggregation, and the short guard interval for 11n network traffic.

Definitions of terms used in syntax:

- **Aggregate MAC Protocol Data Unit (A-MPDU)** — Allows multiple MPDUs to be transmitted as a single PDU frame.
- **Aggregate MAC Service Data Unit (A-MSDU)** — Allows multiple MSDUs to be transmitted within a single or multiple data MSDUs. Only MSDUs whose destination address and source address map to the same receiver address and transmitter address are aggregated.
- **Short Guard Interval** — Used to prevent inter-symbol interference for 802.11n. When enabled, the interval is 400 nanoseconds and it enhances throughput when multipath delay is low.

**Syntax** —

```plaintext
set service-profile name 11n a-mpdu-max-length [8K | 16K | 32K | 64K] a-msdu-max-length [4K | 8K] frame-aggregation [mdmu | mpdu | all | disable] {mode-na | mode-ng [enable | disable | required]} short-guard-interval [enable | disable]
```

- **a-mpdu-max-length** — Configures the length of the MPDU packet in kilobytes. Select from 8, 16, 32, or 64K.
- **a-msdu-max-length** — Configures the length of the MSDU packet in kilobytes. Select from 4 or 8K.
- **frame-aggregation** — Enables aggregation of MPDU and MSDU packets. Select either MPDU or MSDU or all. You can also disable this option.
- **short-guard-interval** — Configure this option to prevent inter-symbol interference on the 802.11n network.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 7.0.

set service-profile transmit-rates

Configures the data rates supported by MAP radios for a service-profile SSID. This is an existing command. The only change in MSS 7.0 is to add support and transmit rates for 11ng and 11na.
**External Captive Portal Support**

The ability to redirect Web portal authentication to a Web server on a network rather than a local WX database or RADIUS is now available in MSS 7.0. For more information on this function, refer to the *Wireless LAN Switch and Controller Configuration Guide*.

The following MSS command supports this function:

```
WX# set service-profile profile-name web-portal-form URL
```
Simultaneous Login Support

You can now limit the number of concurrent sessions that a user can have on the network. You can use the vendor-specific attribute (VSA) on a RADIUS server or configure it as part of a service profile. You can apply the attribute to users and user groups.

The attribute, `simultaneous-logins`, has been added to the following commands:

- `set user username attr simultaneous-logins value`
- `set usergroup group-name attr simultaneous-logins value`
- `set service-profile name attr simultaneous-logins value`

where `value` is between 0-1000. In the case of the `set user attr` command, if you set the value to 0, then the user is locked out of the network. The default value is unlimited access. In addition, setting this value applies only to user sessions in the mobility domain and not a specific WX.

To clear the configuration, use one of the following commands:

- `clear user username attr simultaneous-logins`
- `clear usergroup group-name attr simultaneous-logins`

Dynamic RADIUS Extensions

These commands and attributes support configuration of dynamic RADIUS extensions per RFC 3576 (Dynamic Authorization Server MIB).

- `set radius dac` Configures dynamic RADIUS extensions in support of RFC 3576.

  **Syntax** — `set radius dac name ip-addr key string [disconnect [enable | disable] | [change-of-author [enable | disable] | replay-protection [enable | disable] | replay-window seconds]`

  **Defaults** — None.

  **Access** — Enabled.

  **History** — Introduced in MSS Version 6.2.

- `set radius das-port` Configures the dynamic authorization port for dynamic RADIUS servers.

  **Syntax** — `set radius das-port port_number`

  **Defaults** — None.
Access — Enabled.

History — Introduced in MSS Version 6.2.

Examples —

WX# set radius das-port 65539
success:change accepted

clear radius das-port

Clears a configured dynamic RADIUS server authorization port.

Syntax — clear radius das-port port_number

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.2.

Examples — To clear a dynamic RADIUS server port of 3799, use the following command:

WX# clear radius das-port 3799

set authorization dynamic

Configures SSIDs for dynamic RADIUS clients.

Syntax — set authorization dynamic {ssid [wireless_8021X | 8021X | any | name] | wired name}

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.2.

Examples — To configure an SSID named dac_clients, use the following command:

WX# set authorization dynamic ssid dac_clients
success:change accepted

termination-action Attribute

The termination-action dynamic RADIUS attribute is now supported in MSS 7.0. The attribute has been added to the following commands:

set user username attr termination-action value
**NEW FEATURES SUMMARY**

*set usergroup group-name attr termination-action value*

where *value* is 0 or 1. This attribute supports reauthentication of all access types: dot1x, web-portal, MAC, and last-resort. When the value is set to 0, the user session is terminated after the session expires. If the value is set to 1, the user session is reauthenticated by sending a RADIUS request message after the session expires.

**MAC User Range Authentication**

Version 7.0 modifies the User MAC Address field in the existing *set mac-user* and *set mac-user attr* commands to allow input such as `00:11:00:*` instead of just a single MAC address. Only one `*` (asterisk) is allowed in the address format and it must be the last character.

During authentication of the MAC User client, the most specific entry that matches the MAC-user glob is selected. Therefore, an entry for `00:11:30:21:ab:cd` overrides an entry for `00:11:30:21:*`, and an entry for `00:11:30:21:*` overrides an entry for `00:11:30:*`.

To configure a MAC User Range with MSS, use these commands:

```
set mac-user 00:11:*  
set mac-user 00:11:* attr attribute-name value  
set mac-user 00:11:* [group group_name]
```

To configure this feature for authentication on a RADIUS server, use the new command *set authentication mac-prefix* (see the next section).

**set authentication mac-prefix**

Specifies the MAC address prefix for SSID authentication.

**Syntax** — `set authentication mac-prefix {ssid | any} wired mac-glob`

- `mac-glob` — Represents the range of MAC addresses for this rule and determines the prefix used for authentication. During authentication, the MAC prefix is extracted from the MAC-glob and used as the user-name in the Access-Request portion of the handshake.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 7.0.
Usage — You can configure different authentication methods for different groups of MAC addresses by “globbing.”

Examples — To set the MAC address glob for authenticating an SSID, use the following command:

```
WX# set authentication mac-prefix ssid any 00:00*
success: change accepted.
```

### MAC Authentication Request Format

A new parameter, `mac-addr-format`, is available in the `set radius server` command to configure a MAC address format to be sent as a username to a RADIUS server for MAC authentication.

To configure the MAC address format with MSS, use the following command:

```
WX# set radius server name mac-addr-format {hyphens | colons | one-hyphen | raw}
```

For example:

```
WX# set radius server sp1 mac-addr-format ?
  hyphens 12-34-56-78-9a-bc
  colons 12:34:56:78:9a:bc
  one-hyphen 123456-789abc
  raw 123456789abc
```

You can also configure all RADIUS servers to use a specific MAC address format with the following command:

```
WX# set radius mac-addr-format {hyphens | colons | one-hyphen | raw}
```

### User Attribute Enhancements

The RADIUS standard (RFC 2865) allows the attribute `user-name` to be returned as part of the access-accept handshake. The `user-name` string is used as the user-name for the session. MSS supports this functionality on the RADIUS server but not the WX local database. With the release of MSS and 3WXM Version 7.0, this attribute is now supported as part of the login session.

The attribute has been added to the following commands:

```
set user username attr user-name value
```
set mac-user mac-addr attr user-name value
set usergroup group-name attr user-name value
set mac-usergroup group-name attr user-name value

where value is the username that is displayed in session information. It can be up to 80 characters, including numbers and special characters.

To clear the configuration, use one of the following commands:

clear user username attr user-name
clear usergroup group-name attr user-name
clear mac-usergroup group-name attr user-name

If configured, usernames are now part of display output such as display sessions:

WX# display sessions

<table>
<thead>
<tr>
<th>User Name</th>
<th>Sess ID</th>
<th>IP or MAC Address</th>
<th>VLAN</th>
<th>Port/Radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>engineering-05:0c:78</td>
<td>28*</td>
<td>10.7.255.2</td>
<td>yellow</td>
<td>5/1</td>
</tr>
<tr>
<td>engineering-79:86:73</td>
<td>29*</td>
<td>10.7.254.3</td>
<td>red</td>
<td>2/1</td>
</tr>
<tr>
<td>engineering-1a:68:78</td>
<td>30*</td>
<td>10.7.254.8</td>
<td>red</td>
<td>7/1</td>
</tr>
<tr>
<td>engineering-45:12:34</td>
<td>35*</td>
<td>10.9.254.7</td>
<td>blue</td>
<td>2/1</td>
</tr>
</tbody>
</table>

Since the session user name is replaced by the user-name attribute, the display sessions output displays this attribute as the user name for the session. When the attribute is obtained from a user group, the user name of all users in the group appears the same and you cannot differentiate between them. However, the MAC address is added to the user group name in the output.

---

Enhancements to Location Policy Configuration

MSS Version 7.0 adds a time-of-day attribute to the following command for controlling wireless access during certain times of day:

set location policy {deny | permit} if [time-of-day operator time-of-day]

- operator
  - eq - Defines a specific timeframe
  - neq - Defines any time other than a specific timeframe
- time-of-day
**RADIUS Ping Utility**

A command provides a diagnostic tool to enhance troubleshooting capabilities for RADIUS servers on the network.

**radping**

This command sends an authentication request to the RADIUS server to determine if it is offline.

**Syntax** — `radping {server | servername | group servergroup} request [acct-off | acct-on | acct-start | acct-stop | acct-update | authentication] user username password password auth-type {plain | mschap2}

- `servername` — Name of a RADIUS server configured to perform remote AAA services for WX switches.
- `servergroup` — Name of a RADIUS server group configured to perform remote AAA services for WX switches.
- `acct-off, acct-on, acct-start, acct-stop, acct-update` — Send accounting requests to the RADIUS server to collect and start or stop user statistics.
- `authentication` — Send an authentication request to the RADIUS server.
- `username` — A user name configured on the RADIUS server.
- `password` — The password configured for user.
- `auth type {plain | mschap2}` — Authentication type used by the RADIUS server or server group.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.2.

**Examples** — To verify that a RADIUS server `alpha` with the username `smith5` and password `swordfish` is active on the network, use the following command:

```
WX# radping alpha request authentication user smith5 password swordfish auth-type mschap2
Sending authentication request to server test-27708
(10.20.30.40:1812)
```
To send an accounting request to the RADIUS server, use the following command:

```
WX# radping alpha request acct-start
```

To stop the accounting requests, use the following commands:

```
WX# radping alpha request acct-stop
```

### Unique AP Number Support

MSS 7.0 now allows APs to be numbered from 1 to 9999 on a network. However, there is no change to the maximum number of APs that can be configured on a WX.

This affects the following command:

```
set ap apnum
```

where `apnum` is a number in the range 1-9999.

### Bandwidth Management

Bandwidth management allows you to manage network traffic on your network by configuring certain traffic for higher priority over other traffic—for example, VoIP traffic over normal network traffic. You can configure this feature when you implement QoS profiles. You can configure bandwidth management on a per-SSID, per-user, or queuing weights basis.

The QoS profile contains a set of parameters that are applied to clients to assure a specific service level on the network. A QoS profile is an AAA attribute assigned to a client when the client associates on the network. Prior to this release, some QoS parameters were configured as part of the service profile attributes.

Commands and attributes used to implement bandwidth management are described in the remainder of this section. For more detailed information on use of these commands when configuring bandwidth management, see the New Features Summary section in the *Wireless Switch Manager User Guide*.

**set qos profile** Configures QoS parameters for multiple clients.

**Syntax** — `set qos-profile profile-name [access-category background | best effort | video | voice] [permit | demote]`
Bandwidth Management

[cos static-cos-value] [max-bandwidth max-bw-kb] [use-client-dscp enable | disable]

- **profile-name** — Name of the QoS profile.
- **access-category, background, best-effort, video, voice** — Types of forwarding queues to configure QoS.
- **static-cos-value** — Mark QoS traffic with a specific CoS value from 0 to 7.
- **max-bw-kb** — Configure the bandwidth for the QoS profile, from 0 to 100000 Kbps.
- **use-client-dscp [enable | disable]** — MSS classifies QoS level of IP packets based on a DSCP value. You can specify a number from 0 to 7.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.2.

**set radio-profile weighted-fair-queuing**

Configures a minimum service level for specific radio profiles. Medium time weights determine the relative transmit utilization of the radio between service profiles.

**Syntax** — set radio-profile profile-name weighted-fair-queuing {enable | disable} weight service-profile-name weight

- **profile-name** — Name of the radio profile.
- **weighted-fair-queuing** — Enable or disable weighted fair queuing.
- **service-profile-name** — Name of the service profile to apply weighted queuing.
- **weight** — Configure a weight value from 1 to 100. All profiles with weighted queuing add up to 100.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.2.
Examples — To configure weighted queuing for a radio and service profile, use the following command:

WX# set radio-profile wireless weighted-fair-queuing enable
weight mp_conference 25
success: change accepted.

set service-profile max-bw

Configures the maximum bandwidth for a service profile.

Syntax — set service-profile profile-name max-bw max-bw-kb

- profile-name — Name of the service profile.
- max-bw-kb — Configure a bandwidth from 1-300000 Kbps. 0 = unlimited bandwidth.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 7.0.

Usage — Use this command to configure specific bandwidth requirements for a service profile. Once configured, the service profile can be mapped to a specific radio profile.

clear qos-profile

Clears a QoS profile from the configuration.

Syntax — clear qos-profile profile_name

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.2.

Usage — You can also use clear qos-profile profile_name cos, clear qos-profile profile_name use-client-dscp, and clear qos-profile profile_name max-bw to clear these parameters, respectively.

Examples — To clear a QoS profile with the profile name, best_voice, from the MSS configuration, use the following command:

WX# clear qos-profile best_voice
RF Scanning Enhancements

A new attribute, sentry, is now available to independently configure and control scanning behaviors on radios. For example, a disabled radio does not transmit or receive, and a radio that is scanning, but not providing radio service to clients, is in sentry mode. sentry allows longer dwell times on scanning channels than the enable mode. This attribute has been added to the following commands:

```
set ap apnum radio [1 | 2] mode [enable | sentry | disable]
set radio-profile profile-name mode [enable | sentry | disable]
```

The remainder of this section describes commands used to configure RF scanning.

**set radio-profile rf-scanning mode**

Configures RF scanning on radios running MSS 7.0.

**Syntax** — `set radio-profile profile-name rf-scanning mode [passive | active]`

- **profile-name** — Name of the radio profile.
- **passive** — The radio scans once per predefined time and audits the packets on the wireless network. The default time is 1 second.
- **active** — The radio actively sends probes to other channels and then audits the packets on the wireless network.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.2.

**Examples** — To configure active rf-scanning mode for radio profile gofish, use the following command:

```
WX# set radio-profile gofish rf-scanning mode active
success: change accepted
```
**set radio-profile rf-scanning channel-scope**

Configures the channel scope for RF scanning.

**Syntax** — `set radio-profile profile-name rf-scanning channel-scope [operating | regulatory | all]`

- **profile-name** — Name of the radio profile.
- **regulatory** — Scans and audits regulatory channels for 802.11a or 802.11b/g.
- **operating** — Scans and audits the current channel.
- **all** — Scans and audits all channels on the radio

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.2.

**Examples** — To scan only operating channels on radio profile, gofish, use the following command:

```
WX# set radio-profile gofish rf-scanning channel-scope operating
success: change accepted
```

---

**RF Detection Configuration**

This section describes deprecated, replaced, modified, and new `rfdetect` commands for configuring RF classifications in MSS 7.0.

**Deprecated Commands**

The following commands were deprecated as of MSS 6.2:

- `set rfdetect vendor-list [client | ap]`
- `display rfdetect vendor-list`
- `clear rfdetect vendor-list`
- `set radio-profile profile-name countermeasures configured`
Replaced Commands

The following table lists pre-MSS 7.0 commands that are now obsolete and their MSS 7.0 replacements:

Table 3  RF Detection Commands Replaced in MSS 7.0

<table>
<thead>
<tr>
<th>Old Command Group</th>
<th>Equivalent Replacement Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set rfdetect ignore transmit-mac</code></td>
<td>`set rfdetect neighbor-list [transmit-mac</td>
</tr>
<tr>
<td><code>display rfdetect ignore</code></td>
<td><code>display rfdetect neighbor-list</code></td>
</tr>
<tr>
<td><code>clear rfdetect ignore</code></td>
<td>`clear rfdetect neighbor-list [transmit-mac</td>
</tr>
<tr>
<td><code>set rfdetect attack-list mac</code></td>
<td><code>set rfdetect rogue-list mac-addr</code></td>
</tr>
<tr>
<td><code>display rfdetect attack-list</code></td>
<td><code>display rfdetect rogue-list</code></td>
</tr>
<tr>
<td><code>clear rfdetect attack-list</code></td>
<td>`clear rfdetect rogue-list [mac-addr</td>
</tr>
</tbody>
</table>

Parameters:
- `transmit-mac` or `mac-addr` — Basic service set identifier (BSSID), i.e. a MAC address, of the device in the neighbor list.
- `oui` — Vendor device ID.
- `all` — All devices in the neighbor list.

**set rfdetect ssid-list**

This command has been modified to allow a wildcard for SSID names. Only the changes are shown below:

**Syntax** — `set rfdetect ssid-list [ssid-name | ssid*]`

- `ssid-name` — SSID name you want to add to the permitted SSID list.
- `ssid*` — SSID glob at add to the permitted SSID list.

**set rfdetect classification ad-hoc**

New command used to classify devices as ad-hoc devices on the network.

**Syntax** — `set rfdetect classification ad-hoc [rogue | skip-test]`

- `rogue` — Detects ad-hoc networks and classifies them as rogues.
- `skip-test` — Omit looking for ad-hoc networks and go to the next classification step.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.2.
**Examples** — To configure MSS to detect ad-hoc networks and classify them as rogue devices, use the following command:

```plaintext
WX# set rfdetect classification ad-hoc rogue
```

**set rfdetect classification default**

New command used to configure the default classification of unknown devices on the network.

**Syntax** — `set rfdetect classification default [rogue | suspect | neighbor]`

- `rogue` — Sets the default classification as rogue.
- `suspect` — Sets the default classification as suspect.
- `neighbor` — Sets the default classification as neighbor.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.2.

**Examples** — To configure MSS to detect unknown devices and classify them as rogue devices, use the following command:

```plaintext
WX# set rfdetect classification default rogue
```

**set rfdetect classification seen-in-network**

New command used to configure devices seen on the network as rogue devices.

**Syntax** — `set rfdetect classification seen-in-network [rogue | skip-test]`

- `rogue` — Sets the classification as rogue.
- `skip-test` — Sets the default classification as suspect.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.2.
Examples — To configure MSS to detect devices seen on the network and classify them as rogue devices, use the following command:

WX# set rfdetect classification seen-in-network rogue

set rfdetect classification ssid-masquerade

New command used to configure devices with spoofed SSIDs as rogue devices.

Syntax — set rfdetect classification ssid-masquerade [rogue | skip-test]

- rogue — Sets the classification as rogue.
- skip-test — Sets the default classification as suspect.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.2.

Examples — To configure MSS to detect unknown devices and classify them as rogue devices, use the following command:

WX# set rfdetect classification ssid-masquerade rogue

display rfdetect classification

New command that displays information about the RF detect classifications configured on the network.

Syntax — display rfdetect classification

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.2.

Examples — The following shows the RF detect classification on the WX:

<table>
<thead>
<tr>
<th>User</th>
<th>Rules for Classification</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>If in Rogue list</td>
<td>Rogue</td>
</tr>
<tr>
<td>N</td>
<td>If AP is part of Mobility Domain</td>
<td>Member</td>
</tr>
</tbody>
</table>
NEW FEATURES SUMMARY

In previous releases, the `display aaa` command displayed RADIUS, users, and mac-users configuration on the WX. This command is now deprecated and replaced by the `display radius`, `display user`, `display mac-user`, `display usergroup`, and `display mac-usergroup` commands.

**display radius**

Displays RADIUS configuration information and status.

```
WX# display radius
Radius servers Default Values
Auth-Port=1812 Acct-Port=1813 Timeout=5 Acct-Timeout=5
Retrans=3 Deatime=0 Key=(null) Author-Pass=(null)

Radius Servers

<table>
<thead>
<tr>
<th>Server</th>
<th>IP Address</th>
<th>Auth Port</th>
<th>Acct Port</th>
<th>Time Out</th>
<th>Retry</th>
<th>Dead Time</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>rs1</td>
<td>172.21.14.30</td>
<td>1812</td>
<td>1813</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>UP</td>
</tr>
<tr>
<td>rs2</td>
<td>1.1.1.1</td>
<td>1812</td>
<td>1813</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>UP</td>
</tr>
<tr>
<td>dummy</td>
<td>172.21.14.31</td>
<td>1812</td>
<td>1813</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>UP</td>
</tr>
</tbody>
</table>

Server groups
SG1:rs1
SG2:dummy

Radius Dynamic Authorization Configuration
Server port: 3799
```
display user

Displays summary or verbose status relating to users or users matching a glob. For user globs, wildcards (*) are allowed at the beginning or end of the string.

WX# display user [name-glob | verbose]

User Name    Status    Group    VLAN
----------    --------    ------    ------
johndoe     disabled   Admin    red
johnsmith   enabled    Admin    red
guest_access disabled   Guests   red

WX# display user *john*

User Name    Status    Group    VLAN
----------    --------    ------    ------
johndoe     disabled   Admin    red
johnsmith   enabled    Admin    red

WX# display user verbose

User name:     johndoe
Status:       disabled
Password:    iforgot(encrypted)
Group:        Admin
VLAN:         red
Password-expires-in:  12 days
Other attributes:
ssid:        trapeze
end-date:    01/08/23-12:00
idle-timeout:  120
acct-interim-interval: 180
User name: johnsmith
Status: enabled
Password: iforgot2(encrypted)
Group: Admin
VLAN: red
Password.expires-in: 12 days
Other attributes:
None
User name: guest_access
Status: disabled
Password: iforgot3(encrypted)
Group: Admin
VLAN: red
Password.expires-in: 5 days
Other attributes:
ssid: trapeze1
date: 01/08/20-9:00
idle-timeout: 100
acct-interim-interval: 600

WX# display user *john* verbose

User name: johndoe
Status: disabled
Password: iforgot(encrypted)
Group: Admin
VLAN: red
Password.expires-in: 12 days
Other attributes:
ssid: trapeze
date: 01/08/23-12:00
idle-timeout: 120
acct-interim-interval: 180
User name: johnsmith
Status: enabled
display mac-user: Displays summary or verbose status relating to a specific mac-user or all mac-users.

WX# display mac-user [mac-glob | verbose]

<table>
<thead>
<tr>
<th>MAC</th>
<th>Group</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:11:11:21:11:12</td>
<td>Guests</td>
<td>insecure</td>
</tr>
<tr>
<td>00:11:11:21:11:*</td>
<td>Guests</td>
<td>red</td>
</tr>
</tbody>
</table>

WX# display mac-user 00:11:11:21:11:12

<table>
<thead>
<tr>
<th>MAC</th>
<th>Group</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:11:11:21:11:12</td>
<td>Guests</td>
<td>insecure</td>
</tr>
</tbody>
</table>

WX# display mac-user verbose

MAC: 00:11:11:21:12
Group: Guests
VLAN insecure
Other attributes:
ssid: trapeze
der-date: 01/08/23-12:00
idle-timeout: 120
acct-interim-interval: 180
MAC: 00:11:11:21:*
Group: Guests
VLAN insecure
Other attributes:
ssid: trapeze
der-date: 01/08/23-12:00
Idle-timeout: 120
acct-interim-interval: 180

WX# display mac-user 00:11:11:21:11* verbose

MAC: 00:11:11:21:*
Group: Guests
VLAN: insecure
Other attributes:
ssid: trapeze
end-date: 01/08/23-12:00
idle-timeout: 120
acct-interim-interval: 180

**display usergroup** Displays summary status for all user groups or verbose status for a specific user group.

**WX# display usergroup [ug-name]**

<table>
<thead>
<tr>
<th>Usergroup</th>
<th>Users Mapped to Group</th>
<th>VLAN</th>
<th>Other Attr. of Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>2</td>
<td>red</td>
<td>4</td>
</tr>
<tr>
<td>Guests</td>
<td>1</td>
<td>red</td>
<td>2</td>
</tr>
<tr>
<td>Guests2</td>
<td>0</td>
<td>blue</td>
<td>0</td>
</tr>
</tbody>
</table>

**WX# display usergroup Admin**

Usergroup: Admin
VLAN: red
Password-expires-in: 12 days
Other attributes:
ssid: trapeze
end-date: 01/08/23-12:00
idle-timeout: 120
acct-interim-interval: 180
Users in this group:

<table>
<thead>
<tr>
<th>User Name</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>johndoe</td>
<td>red</td>
</tr>
<tr>
<td>johnsmith</td>
<td>red</td>
</tr>
</tbody>
</table>

WX# display usergroup Guests2

Usergroup: Guests2
VLAN: blue
Other attributes:
None

No users in this group.

display mac-usergroup

Displays summary status for all MAC user groups or verbose status for a specific MAC user group.

WX# display mac-usergroup [mac-ug-name | verbose]

<table>
<thead>
<tr>
<th>MAC Usergroup</th>
<th>Users Mapped to Group</th>
<th>VLAN</th>
<th>Other Attr. of Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>0</td>
<td>red</td>
<td>3</td>
</tr>
<tr>
<td>Guests</td>
<td>2</td>
<td>insecure</td>
<td>4</td>
</tr>
</tbody>
</table>

WX# display mac-usergroup Guests

MAC Usergroup: Guests2
VLAN: blue
Other attributes:
ssid: trapeze
date: 01/08/23-12:00
idle-timeout: 120
acct-interim-interval: 180
MAC users in this group:

<table>
<thead>
<tr>
<th>MAC</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:11:11:21:11:12</td>
<td>insecure</td>
</tr>
<tr>
<td>00:11:11:21:11:*</td>
<td>red</td>
</tr>
</tbody>
</table>

WX# display mac-usergroup Admin

MAC Usergroup: Admin
VLAN: red
Other attributes:
ssid: trapeze
idle-timeout: 120
acct-interim-interval: 180

No MAC users in this group.

**display ap config Enhancements**

New commands and output now allow you to see AP configurations on your network.

**display ap config**
Displays a summary of all APs configured on the network.

<table>
<thead>
<tr>
<th>AP</th>
<th>AP Name</th>
<th>Model</th>
<th>Mode</th>
<th>Radio 1 profile</th>
<th>Radio 2 profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td></td>
<td></td>
<td>disabled</td>
<td>default</td>
<td>default</td>
</tr>
<tr>
<td>3</td>
<td>AP03</td>
<td>AP-3750</td>
<td>default</td>
<td></td>
<td>aaaaaaaaaa123456</td>
</tr>
</tbody>
</table>

**display ap config verbose**
Displays all attributes of all APs.

AP 2

Model: AP-3750
Mode: high
Bias: upgrade-firmware, force-image-download, blink
Option: port 2
Serial number: 123456789
Fingerprint: finger_print
Communication timeout: 10 seconds
Location: USA
Contact: contact_name
Vlan-profile:
Radio 1 (11a)
Mode: enabled Radio profile: default
Channel: 36 Load balancing: Yes
Tx power: 13 Load balancing group: heavy_traffic
Auto tune max power: default Force rebalance: no
Antenna location: outdoors Antenna type: ANT5060
Service-profile:
clear-service
Radio 2 (11g)
Mode: enabled Radio profile: default
Channel: 36 Load balancing: enabled
Tx power: 13 Load balancing group: heavy_traffic
Auto tune max power: default Force rebalance: no
Antenna location: outdoors Antenna type: ANT5060
Service-profile:
clear-service
clear-service2 (bridge)

display ap config Displays all attributes of the specified AP.
WX# display ap config apnum
display ap config radio Displays all attributes of the specified AP and specified radio.
WX# display ap config apnum radio [1 | 2]
display load Enhancements Changes to the display load command allow you to obtain instantaneous CPU and memory load information in a more useful format. In addition, more information is provided to assist with troubleshooting the WX on the network.
The following information is displayed:

- **System CPU load**
  Summary data displayed:
  - Last second (also called instant load)
  - Last minute
  - Last 5 minutes
  - Last hour
  - Last day
  - Last three days
  Historical values drawn as a graph, showing peaks and averages:
  - Last minute
  - Last hour
  - Last three days

- **System memory load**
  Summary data displayed:
  - Last second (also called instant load)
  - Last minute
  - Last 5 minutes
  - Last hour
  - Last day
  - Last three days
  Historical values drawn as a graph, showing peaks and averages:
  - Last minute
  - Last hour
  - Last three days

**display load memory**

Output example:

<table>
<thead>
<tr>
<th>Period</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last second:</td>
<td>38456 KB</td>
</tr>
<tr>
<td>Last minute:</td>
<td>38452 KB</td>
</tr>
<tr>
<td>Last 5 minutes:</td>
<td>38048 KB</td>
</tr>
</tbody>
</table>
Last hour: 38486 KB
Last day: 40708 KB
Last 3 days: 40931 KB
Total system memory: 131072 KB

display load cpu

Output example:

<table>
<thead>
<tr>
<th>Period</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last second:</td>
<td>2%</td>
</tr>
<tr>
<td>Last minute:</td>
<td>2%</td>
</tr>
<tr>
<td>Last 5 minutes:</td>
<td>2%</td>
</tr>
<tr>
<td>Last hour:</td>
<td>2%</td>
</tr>
<tr>
<td>Last day:</td>
<td>1%</td>
</tr>
<tr>
<td>Last 3 days:</td>
<td>33141%</td>
</tr>
</tbody>
</table>
display load cpu history

Output example:

| 100 |
| 90  |
| 80  |
| 70  |
| 60  |
| 50  |
| 40  |
| 30  |
| 20  |

^ ^ ^ ^ ^ ^ ^ ^ ^ ^

****************************************************************************

6-----4-----4-----3-----2-----2-----1-----1-----5-----0-----

0 5 0 5 0 5 0 5 0 0

CPU load history for the past hour

* = average CPU load (%)  ^ = peak CPU load (%)

MX# show load memory history

| 128 |
| 112 |
| 106 |
| 96  |
| 80  |
| 64  |
| 48  |

****************************************************************************

****************************************************************************

6-----3-----3-----3-----2-----2-----1-----1-----5-----0-----

0 5 0 5 0 5 0 5 0 0

Memory utilization history for the past hour

* = average utilization (MBytes)  ^ = peak utilization (MBytes)

display radio-profile

The **display radio-profile** command is used to display attributes assigned to a radio. The output of the command is now reformatted to accommodate additional features in MSS 7.0.

Enhancements
**display radio-profile**

Displays all configured attributes of the specified radio profile.

```
WX# display radio-profile default2
```

**Options**

**802.11:** Long-preamble, WMM-power save, Fair-queuing, Rate-enforcement

**QoS:**

Auto tune: Channel-config, Ignore-clients, Power-config

RF-scanning: CTS-to-self

Other: RFID-mode

**802.11**

Beacon Interval: 100
DTIM interval: 1
RTS threshold: 2346

**Auto tune**

Tune channel range: lower-bands
Tune channel interval: 3600
Channel holddown: 300

**RF-scanning**

Mode: ACTIVE
Channel-scope: REGULATORY

**Other**

Countermeasures: None
DFS channels: disabled
QoS mode: wmm

**Queue**

<table>
<thead>
<tr>
<th></th>
<th>ACM</th>
<th>Max %</th>
<th>Police</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>NO</td>
<td>0</td>
<td>YES</td>
</tr>
<tr>
<td>BestEffort</td>
<td>NO</td>
<td>0</td>
<td>YES</td>
</tr>
<tr>
<td>Video</td>
<td>NO</td>
<td>0</td>
<td>YES</td>
</tr>
<tr>
<td>Voice</td>
<td>NO</td>
<td>0</td>
<td>YES</td>
</tr>
</tbody>
</table>

*The information under QoS mode is displayed only if QoS mode is configured for WMM.*
**display sessions network ap enhancements**

New commands and output now allow you to see AP statistics of a network session. The new commands are as follows:

- `display sessions network ap apnum`
- `display sessions network ap apnum verbose`
- `display sessions network ap apnum qos-stats`
- `display sessions network ap apnum radio radionum`
- `display sessions network ap apnum radio radionum verbose`
- `display sessions network ap apnum radio radionum qos-stats`

Output for selected commands is shown below.

**display sessions network ap**

Output example:

```
WX# display sessions network ap 1,7,8
8 of 18 sessions matched
AP 1, conference room

<table>
<thead>
<tr>
<th>User Name</th>
<th>Sess</th>
<th>Address</th>
<th>VLAN</th>
<th>Radio</th>
<th>Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>last-resort-user1</td>
<td>2*</td>
<td>172.17.55.166 user-vlan</td>
<td>2</td>
<td>11a</td>
<td></td>
</tr>
<tr>
<td>last-resort-user2</td>
<td>5*</td>
<td>172.17.55.166 user-vlan</td>
<td>1</td>
<td>11bg</td>
<td></td>
</tr>
<tr>
<td>last-resort-user3</td>
<td>10*</td>
<td>172.17.55.167 user-vlan</td>
<td>2</td>
<td>11a</td>
<td></td>
</tr>
<tr>
<td>last-resort-user4</td>
<td>12*</td>
<td>172.17.55.168 user-vlan</td>
<td>1</td>
<td>11bg</td>
<td></td>
</tr>
</tbody>
</table>
```

AP 7, kitchen

```
<table>
<thead>
<tr>
<th>User Name</th>
<th>Sess</th>
<th>Address</th>
<th>VLAN</th>
<th>Radio</th>
<th>Band</th>
</tr>
</thead>
<tbody>
<tr>
<td>last-resort-user5</td>
<td>22*</td>
<td>172.17.55.175 user-vlan</td>
<td>2</td>
<td>11a</td>
<td></td>
</tr>
<tr>
<td>last-resort-user6</td>
<td>25*</td>
<td>172.17.55.176 user-vlan</td>
<td>1</td>
<td>11bg</td>
<td></td>
</tr>
<tr>
<td>last-resort-user7</td>
<td>26*</td>
<td>172.17.55.177 user-vlan</td>
<td>2</td>
<td>11a</td>
<td></td>
</tr>
<tr>
<td>last-resort-user8</td>
<td>27*</td>
<td>172.17.55.178 user-vlan</td>
<td>1</td>
<td>11bg</td>
<td></td>
</tr>
</tbody>
</table>
```

**display sessions network ap radio**

Output examples:

```
WX# display sessions network ap 1 radio 1
2 of 18 sessions matched
AP 1, Conference room

<table>
<thead>
<tr>
<th>User Name</th>
<th>Sess</th>
<th>Address</th>
<th>VLAN</th>
<th>Radio</th>
<th>Band</th>
</tr>
</thead>
</table>
```

clear sessions network Enhancements

New `clear sessions network` commands have the following syntax:

- `clear sessions network ap apnum`
- `clear session networks ap apnum radio radionum`

The `apnum` parameter can be specified as one of the following:

- A number - for example, 1.
- A number list - for example, 1,2,7,9 to show sessions on the specified APs.
- A number interval - for example, 1-10, 12-14 displays sessions on APs 1, 2, 3...10 and 12, 13, and 14.

The specified number is limited to the maximum number of supported APs on the WX.

display service-profile Enhancements

The `display service-profile` command is used to display attributes of a given service profile. Several changes are now in place to allow you to easily view the attributes of each configured service profile.
There are two possible forms for the `display service-profile` command:

- `display service-profile name`
- `display service-profile name area area_name`

where `name` is the service profile name and `area_name` is one of the following formats:

- `general`
- `options`
- `crypto`
- `ssid`
- `wep`
- `web-portal`
- `soda`
- `misc`
- `802.11`

The attributes of a service-profile are grouped into nine different areas (attributes). The display format of the output is as follows:

<table>
<thead>
<tr>
<th>General attributes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID name:</td>
<td>string</td>
</tr>
<tr>
<td>SSID type:</td>
<td>string</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options List</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth</td>
<td>{fallthrough (none</td>
</tr>
<tr>
<td>Mesh</td>
<td>{Bridge, Mesh}</td>
</tr>
<tr>
<td>CAC</td>
<td>{CAC, load-balance-exempt}</td>
</tr>
<tr>
<td>L2</td>
<td>{No-broadcast, Proxy-ARP, keep-initial-VLAN}</td>
</tr>
<tr>
<td>802.11</td>
<td>{Beacon, Idle-client-probing}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Crypto</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>{802.1X. PSK, Shared-key}</td>
</tr>
<tr>
<td>Encryption</td>
<td>{RSN, WPA}</td>
</tr>
<tr>
<td>Cipher</td>
<td>{CCMP, TKIP, WEP40, WEP104}</td>
</tr>
<tr>
<td>Pre-shared key</td>
<td>string*</td>
</tr>
<tr>
<td>SSID</td>
<td></td>
</tr>
<tr>
<td>Vlan Name</td>
<td>string*</td>
</tr>
<tr>
<td>Feature</td>
<td>Type</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Encryption type</td>
<td>string*</td>
</tr>
<tr>
<td>End date</td>
<td>string*</td>
</tr>
<tr>
<td>Filter ID</td>
<td>string [, string]*</td>
</tr>
<tr>
<td>Idle timeout</td>
<td>string*</td>
</tr>
<tr>
<td>Mobility profile</td>
<td>string*</td>
</tr>
<tr>
<td>Qos profile</td>
<td>string*</td>
</tr>
<tr>
<td>Service type</td>
<td>string*</td>
</tr>
<tr>
<td>Session timeout</td>
<td>string*</td>
</tr>
<tr>
<td>Start date</td>
<td>string*</td>
</tr>
<tr>
<td>URL:</td>
<td>string*</td>
</tr>
<tr>
<td>WEP</td>
<td></td>
</tr>
<tr>
<td>Active-unicast-index</td>
<td>int 1...4</td>
</tr>
<tr>
<td>Active-multicast-index</td>
<td>int 1...4</td>
</tr>
<tr>
<td>Preset keys</td>
<td>(int...4)</td>
</tr>
<tr>
<td>Web Portal</td>
<td></td>
</tr>
<tr>
<td>ACL</td>
<td>string*</td>
</tr>
<tr>
<td>Form</td>
<td>string*</td>
</tr>
<tr>
<td>Logout mode</td>
<td>enabled</td>
</tr>
<tr>
<td>Logout URL</td>
<td>string*</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>string*</td>
</tr>
<tr>
<td>SODA</td>
<td></td>
</tr>
<tr>
<td>Agent directory</td>
<td>string*</td>
</tr>
<tr>
<td>Enforce checks</td>
<td>enabled</td>
</tr>
<tr>
<td>Failure page</td>
<td>string*</td>
</tr>
<tr>
<td>Remediation ACL</td>
<td>string*</td>
</tr>
<tr>
<td>Success Page</td>
<td>string*</td>
</tr>
<tr>
<td>Logout Page</td>
<td>string*</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td></td>
</tr>
<tr>
<td>CAC Session</td>
<td>int 0...500</td>
</tr>
<tr>
<td>Short Retry Counter</td>
<td>int 1...15</td>
</tr>
<tr>
<td>Long Retry Count</td>
<td>int 1...15</td>
</tr>
<tr>
<td>Max Bandwidth</td>
<td>int 1...100000 Kbps</td>
</tr>
<tr>
<td>User Idle Timeout</td>
<td>int 20...86400</td>
</tr>
<tr>
<td>802.11 Settings</td>
<td>11a</td>
</tr>
</tbody>
</table>
**NEW FEATURES SUMMARY**

- option present only if a value is set

The Options list displays only enabled attributes.

**Output example:**

```
WX# display service-profile sp-1
```

**General attributes**

SSID Name: sp-1  
SSID Type: clear

Options list
Auth: Fallthru none, DHCP-restrict, SODA  
Mesh: Mesh, Bridge  
CAC: CAC, Load-balance-exempt  
L2: No-broadcast, Proxy-ARP, Keep-initial-vlan  
802.11: Beacon

**Crypto attributes**
Authentication: 802.1X, PSK, Shared-key  
Encryption: RSN, WPA  
Cipher: CCMP, TKIP (countermeasures time 30000 ms), WEP40, WEP104
Pre-shared-key: e647c43e9a166bb15724384b5b57f98c664dbe2069aaa1352ec1d28dacb1975

SSID attributes
Filter id: traffic.in, filter.out
Mobility profile: mob-pro
Service type: 2
Start date: 06/06/07, 12:38
End date: 06/12/07, 00:00
Time of day: su0800-2000
Session timeout: 8000
Idle timeout: 600
URL: http://test.com/index.html

WEP attributes
Active-unicast-index: 2
Active-multicast-index: 1
Preset keys: 1,2,4

Web-Portal attributes
ACL: acl-test
Session timeout: 5
Logout mode: disabled
Form: web-portal-login

SODA attributes
Enforce SODA checks: enabled
Remediation ACL: acl-soda1
Success web-page: web-success-soda
Failure web-page: web-fail-soda
Logout web-page: web-logout-soda
Agent directory: agent-soda-dir

Miscellaneous attributes
CAC sessions: 8
Max bandwidth: 3000 kb/s
User idle timeout: 180

802.11 settings

11a
Beacon rate: 6
Multicast rate: auto
Mandatory rate: 6, 12, 24
Standard rates: 9, 18, 36, 48, 54
NEW FEATURES SUMMARY

11b
Beacon rate: 2
Multicast rate: auto
Mandatory rates: 1, 2
Standard rates: 5.5, 11

11g
Beacon rate: 2
Multicast rate: auto
Mandatory rates: 1, 2, 5.5, 11
Standard rates: 6, 9, 12, 18, 24, 36, 48, 54

display rfdetect
Changes
The display rfdetect command is updated in MSS 7.0 and allows you to specify options to narrow down the display output.

Deprecated Commands
The following commands are deprecated in MSS 7.0:
- display rfdetect visible
- display rfdetect clients

display rfdetect data
This command has been simplified in MSS 7.0 — the number of items displayed by the command has been reduced.
display rfdetect data bssid macglob | vendor vendor-name | class [none | member | neighbor | suspect | rogue] clients [mac macglob | ap macglob ap-number-list] | [radio radio-number | adhoc | tag | unknown] [verbose | summary]

Output example:
WX# display rfdetect data
Total number of entries: 13

Detected BSSID Vendor Class AP Name Ch RSSI Age SSID
00:0b:0e:09:1e:41 Trapeze suspt AP02 149 -62 198 rack3-guest-11b
00:0b:0e:09:28:00 Trapeze none AP02 11 -53 33 silviu-ssud-4
00:0b:0e:09:28:01 Trapeze none AP02 36 -59 18 wpa2pmk
00:0b:0e:0a:32:80 Trapeze suspt AP02 6 -78 3 trapezewlan_psk
00:0b:0e:0a:32:81 Trapeze suspt AP02 36 -76 63 trapezewlan_psk
00:0b:0e:0a:32:82 Trapeze suspt AP02 6 -76 78 trapezewlan
You can further refine the output using the options listed below:

**bssid**
The entire BSSID in the format XX:XX:XX:XX:XX:XX or in a macglob format consisting of a subset of the BSSIDs. The subset can be from 1 to 5 bytes of data, for instance, 01:02:03:04 displays all records beginning with those bytes.

**WX# display rfDetect data [bssid | bssid**

**vendor-name**
Display by vendor name.

**WX# display rfDetect data vendor vendor-name**

**SSID**
Can be specified as a string or glob with the format ssid-name for the full name and ssid* to match all SSIDs beginning with SSID.

**WX# display rfDetect data ssid**
Total number of entries: 13

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Vendor</th>
<th>Class</th>
<th>AP Name</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:0e:09:1e:41</td>
<td>Trapeze</td>
<td>suspt</td>
<td>AP02</td>
<td>149</td>
<td>-62</td>
<td>198</td>
</tr>
<tr>
<td>00:0b:0e:09:28:00</td>
<td>Trapeze</td>
<td>none</td>
<td>AP02</td>
<td>11</td>
<td>-53</td>
<td>33</td>
</tr>
</tbody>
</table>

SSID: alina_web

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Vendor</th>
<th>Class</th>
<th>AP Name</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:0e:0a:32:80</td>
<td>Trapeze</td>
<td>suspt</td>
<td>AP02</td>
<td>6</td>
<td>-78</td>
<td>3</td>
</tr>
<tr>
<td>00:0b:0e:0a:32:81</td>
<td>Trapeze</td>
<td>suspt</td>
<td>AP02</td>
<td>36</td>
<td>-76</td>
<td>63</td>
</tr>
</tbody>
</table>

SSID: bedre-pendulum

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Vendor</th>
<th>Class</th>
<th>AP Name</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:0e:0a:32:80</td>
<td>Trapeze</td>
<td>suspt</td>
<td>AP02</td>
<td>6</td>
<td>-78</td>
<td>3</td>
</tr>
<tr>
<td>00:0b:0e:0a:32:81</td>
<td>Trapeze</td>
<td>suspt</td>
<td>AP02</td>
<td>36</td>
<td>-76</td>
<td>63</td>
</tr>
</tbody>
</table>
class
Sort output by classification as a rogue, neighbor, member, suspect, or none.

WX# display rfdetect data class
Total number of entries: 6

class: member

<table>
<thead>
<tr>
<th>Detected BSSID</th>
<th>Vendor</th>
<th>AP Name</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
<th>SSID</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:0e:09:1e:41</td>
<td>Trapeze</td>
<td>AP02</td>
<td>149</td>
<td>-62</td>
<td>198</td>
<td>rde-wpa</td>
<td>part of mob do</td>
</tr>
<tr>
<td>00:0b:0e:09:28:00</td>
<td>Trapeze</td>
<td>AP02</td>
<td>11</td>
<td>-53</td>
<td>33</td>
<td>snmp-radu-</td>
<td>part of mob do</td>
</tr>
</tbody>
</table>

class: suspect

<table>
<thead>
<tr>
<th>Detected BSSID</th>
<th>Vendor</th>
<th>AP Name</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
<th>radu2</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:0e:0a:32:80</td>
<td>Trapeze</td>
<td>AP02</td>
<td>6</td>
<td>-78</td>
<td>3</td>
<td>default</td>
<td>class</td>
</tr>
</tbody>
</table>

WX# display rfdetect data class rogue
5 of 6 entries matched

class: rogue

<table>
<thead>
<tr>
<th>Detected BSSID</th>
<th>Vendor</th>
<th>AP Name</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
<th>SSID</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:0e:09:1e:41</td>
<td>Trapeze</td>
<td>AP02</td>
<td>149</td>
<td>-62</td>
<td>198</td>
<td>rde-wpa</td>
<td>part of mob do</td>
</tr>
<tr>
<td>00:0b:0e:09:28:00</td>
<td>Trapeze</td>
<td>AP02</td>
<td>11</td>
<td>-53</td>
<td>33</td>
<td>snmp-radu-</td>
<td>part of mob do</td>
</tr>
<tr>
<td>00:0b:0e:0a:32:80</td>
<td>Trapeze</td>
<td>AP02</td>
<td>6</td>
<td>-78</td>
<td>3</td>
<td>radu</td>
<td>part of mob do</td>
</tr>
</tbody>
</table>

Values displayed in the Reason column can be any one of the following:

- If the class value is set to None, there are two possible Reason codes:
  - Has not been classified
  - Not enough information to classify

SSID: clear-vlad

Detected BSSID | Vendor | Class | AP Name | Ch | RSSI | Age |
---------------|--------|-------|---------|----|------|-----|
| 00:0b:0e:0a:32:83 | Trapeze | suspt | AP02    | 36 | -76  | 78  |
| 00:0b:0e:0a:bc:00 | Trapeze | suspt | AP02    | 1  | -66  | 33  |
If the class is set to Member, there are two possible Reason codes:

- AP is part of the Mobility Domain
- AP is not part of the Mobility Domain but passes the fingerprint test

If the class is set to Neighbor, there are three possible Reason codes:

- AP is in the Neighbor list
- AP is in the SSID list
- AP is in the Vendor list

If the class is set to Suspect, there are two possible Reason codes:

- List of all unskipped user tests
- Not SSID-spoof; not seen in network; not in Vendor-list

If the class is set to Rogue, there are six possible Reason codes:

- In Rogue list
- SSID spoof
- Seen in the network
- Ad hoc device
- Not in SSID list
- Not in Vendor list

**display rfdetect data ap**

The output for the *display rfdetect data ap* command is sorted by AP number, radio band, and then by detected BSSID.

Output example:

```
WX# display rfdetect data ap 1-6

5 of 13 entries matched

AP: 1 - Room-237
Detected BSSID  Vendor  Ch  Class  RSSI  Age  SSID
------------------  ------  --  -----  ----  ---  ----
00:0b:0e:09:1e:41  Trapeze  149 rogue  -62  198  rde-wpa
00:0b:0e:09:28:00  Trapeze  11 rogue  -53  33   snmp-radu-lung
00:0b:0e:0a:32:80  Trapeze   6 membr  -78   3   radu
00:0b:0e:09:1e:42  Trapeze  149 membr  -62  198  rde-wpa
```

AP: 2 - AP02
**NEW FEATURES SUMMARY**

**display rf detect data clients**

This command can be used to display client data in two ways: generic, and based on the MAC address of the AP connected to the client.

```
WX# display rf detect data clients
Total number of entries: 5
```

Detected BSSID | Vendor | Ch | Class | RSSI | Age | SSID
--- | ------ | --- | ----- | ---- | --- | ----
00:0b:0e:09:1e:42 | Trapeze | 149 | suspt | -62 | 198 | rde-wpa

```
WX# display rf detect data clients ap 00:0b:0e
4 or 5 entries matched
```

Connected BSSID | Detected Client | Vendor | Class | Connected BSSID | AP Name | Ch | RSSI | Age
--- | --------------- | ------ | ----- | --------------- | ------- | --- | ---- | ---
00:0b:0e:2c:c8:41 | 00:0e:35:ca:d2:5f | Intel | suspt | 00:0b:0e:2c:c8:41 | AP01 | 149 | -62 | 198
00:0b:0e:2f:9b:c4 | 00:0f:b5:86:cc:54 | Netgear | rogue | unknown | AP01 | 11 | -53 | 33
00:0b:0e:2f:9b:c4 | 00:0f:b5:86:cc:54 | Netgear | memb | 00:0b:0e:2f:9b:c4 | AP01 | 6 | -78 | 3
00:0b:0e:09:1e:42 | D-link | suspt | 00:0b:0e:2f:71:c1 | AP01 | 149 | -62 | 198
00:11:95:87:38:e2 | D-link | suspt | unknown | AP01 | 149 | -62 | 4

```
WX# display rf detect data clients verbose
4 or 5 entries matched
```

Connected BSSID | Detected Client | Vendor | Class | Connected BSSID | AP Name | Ch | RSSI | Age
--- | --------------- | ------ | ----- | --------------- | ------- | --- | ---- | ---
00:0b:0e:2c:c8:41 | 00:0e:35:ca:d2:5f | Intel | suspt | 00:0b:0e:2c:c8:41 | AP01 | 149 | -62 | 198
00:0f:b5:86:cc:54 | 00:0f:b5:86:cc:54 | Netgear | rogue | unknown | AP01 | 11 | -53 | 33
00:0b:0e:2f:71:c1 | 00:0b:0e:2f:9b:c4 | Netgear | memb | 00:0b:0e:2f:9b:c4 | AP01 | 6 | -78 | 3
00:11:95:87:38:e2 | D-link | suspt | unknown | AP01 | 149 | -62 | 4
00:14:6c:a1:b3:b9 | D-link | suspt | 00:11:95:8b:a0:cf | AP01 | 149 | -62 | 198

**display rf detect data verbose**

This command displays additional details about the rf detect configuration and can be used to display more information about client configuration or generic configurations. Up to 3400 rf detect verbose entries can be displayed at one time.

```
WX# display rf detect clients verbose
Total number of entries: 22
```

**Client:** 00:14:6c:a1:b3:b9

**Client vendor:** Netgear

**Class:** Rogue

**Reason:** seen in the network
display rfdetect Changes

Connected BSSID: 00:0b:0e:14:d4:81
BSSID vendor: Trapeze
AP Number: 10
AP Name: room-pn2-1
Radio: 1
Radio band: 11bg
Rate: 54 MB/s
RSSI: -70
Age 584

WX# display rfdetect data ssid Trapeze* verbose
3 of 12 entries matched

BSSID: 01:02:03:04:05:06
SSID: Trapeze_MX20
Class: Member
Reason: In-ignore-list
Type: Infrastructure
Encryption: CCMP, TKIP, WEP40
Vendor: Trapeze
Listeners:

<table>
<thead>
<tr>
<th>AP</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room-237</td>
<td>11</td>
<td>-66</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>Room-238</td>
<td>11</td>
<td>-85</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Room-236</td>
<td>11</td>
<td>-90</td>
<td>15</td>
<td>Trapeze_MX20</td>
</tr>
</tbody>
</table>

BSSID: 01:02:03:04:35:76
SSID: Trapeze_secure
Class: Rogue
Reason: Not-in-Vendor-list
Type: Infrastructure
Encryption: CCMP, TKIP, WEP140
Vendor: Trapeze
Listeners:
**NEW FEATURES SUMMARY**

**display rfdetect data summary**  
This command has two forms: client and general. The client form displays a summary of all detected clients by AP. The general form displays a summary of all rfdetect data by both SSID and Vendor.

**WX# display rfdetect data clients summary**

<table>
<thead>
<tr>
<th>AP</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room-237</td>
<td>11</td>
<td>-66</td>
<td>123</td>
<td>Trapeze_secure</td>
</tr>
<tr>
<td>Room-238</td>
<td>11</td>
<td>-85</td>
<td>15</td>
<td>Trapeze_secure</td>
</tr>
</tbody>
</table>

**BSSID:** 01:02:03:04:35:80  
**SSID:** Rack117-WX-105-Clear  
**Class:** Rogue  
**Reason:** Not-in-SSID-list  
**Type:** Ad-hoc  
**Encryption:** None  
**Vendor:** Trapeze  

<table>
<thead>
<tr>
<th>AP</th>
<th>Ch</th>
<th>RSSI</th>
<th>Age</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Room-237</td>
<td>11</td>
<td>-66</td>
<td>123</td>
<td>Rack117-WX-105-Clear</td>
</tr>
<tr>
<td>Room-238</td>
<td>11</td>
<td>-85</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Room-236</td>
<td>11</td>
<td>-90</td>
<td>15</td>
<td></td>
</tr>
</tbody>
</table>

**AP Name**  
**Radio**  
**susp**  
**Clients**  
**knwn**  
**roge**  
**adh**  
**tag**  
**Last Seen**  

<table>
<thead>
<tr>
<th>AP_Name</th>
<th>Radio</th>
<th>susp</th>
<th>knwn</th>
<th>roge</th>
<th>adh</th>
<th>tag</th>
<th>Last Seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP_Room_211</td>
<td>b/g</td>
<td>5</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>129</td>
</tr>
<tr>
<td></td>
<td>a</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>29</td>
</tr>
<tr>
<td>AP_Room_553</td>
<td>b/g</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>a</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>AP_Room_941</td>
<td>b/g</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>a</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Totals:</th>
<th>=====</th>
<th>=====</th>
<th>=====</th>
<th>=====</th>
<th>=====</th>
<th>=====</th>
<th>=====</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>29</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>129</td>
<td></td>
</tr>
</tbody>
</table>
1 USING THE COMMAND-LINE INTERFACE

This chapter discusses the 3Com Wireless Switch Manager (3WXM) command-line interface (CLI). Described are:

- CLI conventions (see “CLI Conventions” on page 76)
- Editing on the command line (see “Command-Line Editing” on page 81)
- Using the CLI help feature (see “Using CLI Help” on page 83)
- Information about the command descriptions in this reference (see “Understanding Command Descriptions” on page 84)

Overview

Mobility System Software (MSS) operates a 3Com Mobility System wireless LAN (WLAN) consisting of 3Com Wireless Switch Manager (3WXM) software and 3Com Wireless LAN Switch or 3Com Wireless LAN Controller (WX switch) and 3Com Wireless LAN Managed Access Point (MAP) hardware. There is a command-line interface (CLI) on the WX switch that you can use to configure and manage the WX and its attached access points.

You configure the wireless LAN switches and access points primarily with set, clear, and display commands. Use set commands to change parameters. Use clear commands to reset parameters to their defaults. In many cases, you can overwrite a parameter with another set command. Use display commands to show the current configuration and monitor the status of network operations.

The wireless LAN switches support two connection modes:

- Administrative access mode, which enables the network administrator to connect to the WX switch and configure the network
- Network access mode, which enables network users to connect through the WX switch to access the network
CHAPTER 1: USING THE COMMAND-LINE INTERFACE

CLI Conventions

Be aware of the following MSS CLI conventions for command entry:

- “Command Prompts” on page 76
- “Syntax Notation” on page 76
- “Text Entry Conventions and Allowed Characters” on page 77
- “User Globs, MAC Address Globs, and VLAN Globs” on page 78
- “Port Lists” on page 80
- “Virtual LAN Identification” on page 81

Command Prompts

By default, the MSS CLI provides the following prompt for restricted users. The mmmm portion shows the wireless LAN switch model number (for example, 1200).

WXmmmm>

After you become enabled as an administrative user by typing `enable` and supplying a suitable password, MSS displays the following prompt:

WXmmmm#

For information about changing the CLI prompt on a wireless LAN switch, see “set prompt” on page 107.

Syntax Notation

The MSS CLI uses standard syntax notation:

- Bold monospace font identifies the command and keywords you must type. For example:
  
  ```
  set enablepass
  ```

- Italics indicate a placeholder for a value. For example, you replace `vlan-id` in the following command with a virtual LAN (VLAN) ID:

  ```
  clear interface vlan-id ip
  ```

- Curly brackets `{}` indicate a mandatory parameter, and square brackets `[]` indicate an optional parameter. For example, you must enter `dynamic` or `port` and a port list in the following command, but a VLAN ID is optional:

  ```
  clear fdb {dynamic | port port-list} [vlan vlan-id]
  ```
CLI Conventions

A vertical bar (|) separates mutually exclusive options within a list of possibilities. For example, you enter either `enable` or `disable`, not both, in the following command:

```plaintext
set port {enable | disable} port-list
```

Text Entry Conventions and Allowed Characters

Unless otherwise indicated, the MSS CLI accepts standard ASCII alphanumeric characters, except for tabs and spaces, and is case-insensitive.

The CLI has specific notation requirements for MAC addresses, IP addresses, and masks, and allows you to group usernames, MAC addresses, virtual LAN (VLAN) names, and ports in a single command.

3Com recommends that you do not use the same name with different capitalizations for VLANs or access control lists (ACLs). For example, do not configure two separate VLANs with the names `red` and `RED`.

The CLI does not support the use of special characters including the following in any named elements such as SSIDs and VLANs: ampersand (&), angle brackets (< >), number sign (#), question mark (?), or quotation marks (" ").

In addition, the CLI does not support the use of international characters such as the accented É in DÉCOR.

MAC Address Notation

MSS displays MAC addresses in hexadecimal numbers with a colon (:) delimiter between bytes — for example, 00:01:02:1a:00:01. You can enter MAC addresses with either hyphen (-) or colon (;) delimiters, but colons are preferred.

For shortcuts:

- You can exclude leading zeros when typing a MAC address. MSS displays of MAC addresses include all leading zeros.

- In some specified commands, you can use the single-asterisk (*) wildcard character to represent from 1 byte to 5 bytes of a MAC address. (For more information, see “MAC Address Globs” on page 79.)
IP Address and Mask Notation

MSS displays IP addresses in dotted decimal notation — for example, 192.168.1.111. MSS makes use of both subnet masks and wildcard masks.

Subnet Masks

Unless otherwise noted, use classless interdomain routing (CIDR) format to express subnet masks — for example, 192.168.1.112/24. You indicate the subnet mask with a forward slash (/) and specify the number of bits in the mask.

Wildcard Masks

Security access control lists (ACLs) use source and destination IP addresses and wildcard masks to determine whether the wireless LAN switch filters or forwards IP packets. Matching packets are either permitted or denied network access. The ACL checks the bits in IP addresses that correspond to any 0s (zeros) in the mask, but does not check the bits that correspond to 1s (ones) in the mask. You specify the wildcard mask in dotted decimal notation.

For example, the address 10.0.0.0 and mask 0.255.255.255 match all IP addresses that begin with 10 in the first octet.

The ACL mask must be a contiguous set of zeroes starting from the first bit. For example, 0.255.255.255, 0.0.255.255, and 0.0.0.255 are valid ACL masks. However, 0.255.0.255 is not a valid ACL mask.

User Globs, MAC Address Globs, and VLAN Globs

Name “globbing” is a way of using a wildcard pattern to expand a single element into a list of elements that match the pattern. MSS accepts user globs, MAC address globs, and VLAN globs. The order in which globs appear in the configuration is important, because once a glob is matched, processing stops on the list of globs.

User Globs

A user glob is shorthand method for matching an authentication, authorization, and accounting (AAA) command to either a single user or a set of users.

A user glob can be up to 80 characters long and cannot contain spaces or tabs. The double-asterisk (**) wildcard characters with no delimiter characters match all usernames. The single-asterisk (*) wildcard character matches any number of characters up to, but not including, a delimiter character in the glob. Valid user glob delimiter characters are the at (@) sign and the period (.).
Table 4 gives examples of user globs.

### Table 4  User Globs

<table>
<thead>
<tr>
<th>User Glob</th>
<th>User(s) Designated</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:jose@example.com">jose@example.com</a></td>
<td>User jose at example.com</td>
</tr>
<tr>
<td>*@example.com</td>
<td>All users at example.com whose usernames do not contain periods — for example, <a href="mailto:jose@example.com">jose@example.com</a> and <a href="mailto:tamara@example.com">tamara@example.com</a>, but not <a href="mailto:nin.wong@example.com">nin.wong@example.com</a>, because nin.wong contains a period</td>
</tr>
<tr>
<td>*@marketing.example.com</td>
<td>All marketing users at example.com whose usernames do not contain periods</td>
</tr>
<tr>
<td><em>,.</em>@marketing.example.com</td>
<td>All marketing users at example.com whose usernames contain periods</td>
</tr>
<tr>
<td>*</td>
<td>All users with usernames that have no delimiters</td>
</tr>
<tr>
<td>EXAMPLE*</td>
<td>All users in the Windows Domain EXAMPLE with usernames that have no delimiters</td>
</tr>
<tr>
<td>EXAMPLE*.,*</td>
<td>All users in the Windows Domain EXAMPLE whose usernames contain periods</td>
</tr>
<tr>
<td>**</td>
<td>All users</td>
</tr>
</tbody>
</table>

### MAC Address Globs

A media access control (MAC) address glob is a similar method for matching some authentication, authorization, and accounting (AAA) and forwarding database (FDB) commands to one or more 6-byte MAC addresses. In a MAC address glob, you can use a single asterisk (*) as a wildcard to match all MAC addresses, or as follows to match from 1 byte to 5 bytes of the MAC address:

```
00:*  
00:01:*  
00:01:02:*  
00:01:02:03:*  
00:01:02:03:04:*  
```

For example, the MAC address glob 02:06:8c* represents all MAC addresses starting with 02:06:8c. Specifying only the first 3 bytes of a MAC address allows you to apply commands to MAC addresses based on an organizationally unique identity (OUI).
CHAPTER 1: USING THE COMMAND-LINE INTERFACE

VLAN Glob

A VLAN glob is a method for matching one of a set of local rules on an wireless LAN switch, known as the location policy, to one or more users. MSS compares the VLAN glob, which can optionally contain wildcard characters, against the VLAN-Name attribute returned by AAA, to determine whether to apply the rule.

To match all VLANs, use the double-asterisk (**) wildcard characters with no delimiters. To match any number of characters up to, but not including, a delimiter character in the glob, use the single-asterisk (*) wildcard. Valid VLAN glob delimiter characters are the at (@) sign and the period (.).

For example, the VLAN glob `bldg4.*` matches `bldg4.security` and `bldg4.hr` and all other VLAN names with `bldg4.` at the beginning.

Matching Order for Globs

In general, the order in which you enter AAA commands determines the order in which MSS matches the user, MAC address, or VLAN to a glob. To verify the order, view the output of the `display aaa` or `display config` command. MSS checks globs that appear higher in the list before items lower in the list and uses the first successful match.

Port Lists

The physical Ethernet ports on a WX switch can be set for connection to MAP access points, authenticated wired users, or the network backbone. You can include a single port or multiple ports in one MSS CLI command by using the appropriate list format.

The ports on a WX switch are numbered 1 through 4 (for the 3Com Wireless LAN Controller WX4400) and 1 through 8 (for the 3Com Wireless Lan Switch WX1200). No port 0 exists on the WX switch. You can include a single port or multiple ports in a command that includes `port port-list`. Use one of the following formats for `port-list`:

- A single port number. For example:
  ```
  WX1200# set port enable 6
  ```

- A comma-separated list of port numbers, with no spaces. For example:
  ```
  WX1200# display port poe 1,2,4
  ```
- A hyphen-separated range of port numbers, with no spaces. For example:

  WX1200# reset port 1-3

- Any combination of single numbers, lists, and ranges. Hyphens take precedence over commas. For example:

  WX1200# display port status 1-3,6

Virtual LAN Identification

The names of virtual LANs (VLANs), which are used in Mobility Domain™ communications, are set by you and can be changed. In contrast, VLAN ID numbers, which the wireless LAN uses locally, are determined when the VLAN is first configured and cannot be changed. Unless otherwise indicated, you can refer to a VLAN by either its VLAN name or its VLAN number. CLI set and display commands use a VLAN’s name or number to uniquely identify the VLAN within the WX.

Command-Line Editing

MSS editing functions are similar to those of many other network operating systems.

Keyboard Shortcuts

The following table lists the keyboard shortcuts for entering and editing CLI commands.

<table>
<thead>
<tr>
<th>Keyboard Shortcut(s)</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+A</td>
<td>Jumps to the first character of the command line.</td>
</tr>
<tr>
<td>Ctrl+B or Left Arrow key</td>
<td>Moves the cursor back one character.</td>
</tr>
<tr>
<td>Ctrl+C</td>
<td>Escapes and terminates prompts and tasks.</td>
</tr>
<tr>
<td>Ctrl+D</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Ctrl+E</td>
<td>Jumps to the end of the current command line.</td>
</tr>
<tr>
<td>Ctrl+F or Right Arrow key</td>
<td>Moves the cursor forward one character.</td>
</tr>
<tr>
<td>Ctrl+K</td>
<td>Deletes from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Ctrl+L or Ctrl+R</td>
<td>Repeats the current command line on a new line.</td>
</tr>
<tr>
<td>Ctrl+N or Down Arrow key</td>
<td>Enters the next command line in the history buffer.</td>
</tr>
<tr>
<td>Ctrl+P or Up Arrow key</td>
<td>Enters the previous command line in the history buffer.</td>
</tr>
</tbody>
</table>
History Buffer
The history buffer stores the last 63 commands you entered during a terminal session. You can use the Up Arrow and Down Arrow keys to select a command that you want to repeat from the history buffer.

Tabs
The MSS CLI uses the Tab key for command completion. You can type the first few characters of a command and press the Tab key to show the command(s) that begin with those characters. For example:

WX1200# display i <Tab>
ifm display interfaces maintained by the interface manager
igmp display igmp information
interface display interfaces
ip display ip information

Table 5  Keyboard Shortcuts (continued)

<table>
<thead>
<tr>
<th>Keyboard Shortcut(s)</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+U or Ctrl+X</td>
<td>Deletes characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Ctrl+W</td>
<td>Deletes the last word typed.</td>
</tr>
<tr>
<td>Esc B</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td>Esc D</td>
<td>Deletes characters from the cursor forward to the end of the word.</td>
</tr>
<tr>
<td>Delete key or Backspace key</td>
<td>Erases mistake made during command entry. Reenter the command after using this key.</td>
</tr>
</tbody>
</table>

Single-Asterisk (*)
Wildcard Character
You can use the single-asterisk (*) wildcard character in globbing. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 78.)

Double-Asterisk (**) Wildcard Characters
The double-asterisk (**) wildcard character matches all usernames. For details, see “User Globs” on page 78.
Using CLI Help

The CLI provides online help. To see the full range of commands available at your access level, type the **help** command. For example:

WX1200# **help**

Commands:

- `clear` Clear, use 'clear help' for more information
- `commit` Commit the content of the ACL table
- `copy` Copy from filename (or url) to filename (or url)
- `crypto` Crypto, use 'crypto help' for more information
- `delete` Delete url
- `dir` Show list of files on flash device
- `disable` Disable privileged mode
- `display` Display, use 'display help' for more information
- `exit` Exit from the Admin session
- `help` Show this help screen
- `history` Show contents of history substitution buffer
- `load` Load, use 'load help' for more information
- `logout` Exit from the Admin session
- `monitor` Monitor, use 'monitor help' for more information
- `ping` Send echo packets to hosts
- `quit` Exit from the Admin session
- `reset` Reset, use 'reset help' for more information
- `rollback` Remove changes to the edited ACL table
- `save` Save the running configuration to persistent storage
- `set` Set, use 'set help' for more information
- `telnet` telnet IP address [server port]
- `traceroute` Print the route packets take to network host

For more information on help, see “help” on page 98.

To see a subset of the online help, type the command for which you want more information. For example, to show all the commands that begin with the letter *i*, type the following command:

WX1200# **display i?**

- `ifm` Show interfaces maintained by the interface manager
- `igmp` Show igmp information
- `interface` Show interfaces
- `ip` Show ip information
To see all the variations, type one of the commands followed by a question mark (?). For example:

WX1200# display ip ?
alias       display ip aliases
dns         display DNS status
https       display ip https
route       display ip route table
telnet      display ip telnet

To determine the port on which Telnet is running, type the following command:

WX1200# display ip telnet

<table>
<thead>
<tr>
<th>Server Status</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>23</td>
</tr>
</tbody>
</table>

Understanding Command Descriptions

Each command description in the 3Com Mobility System Software Command Reference contains the following elements:

- A command name, which shows the keywords but not the variables. For example, the following command name appears at the top of a command description and in the index:
  
  \texttt{set ap name}

- A brief description of the command’s functions.

- The full command syntax.

- Any command defaults.

- The command access, which is either enabled or all. All indicates that anyone can access this command. Enabled indicates that you must enter the enable password before entering the command.

- The command history, which identifies the MSS version in which the command was introduced and the version numbers of any subsequent updates.

- Special tips for command usage. These are omitted if the command requires no special usage.

- One or more examples of the command in context, with the appropriate system prompt and response.

- One or more related commands.
This chapter describes access commands used to control access to the Mobility Software System (MSS) command-line interface (CLI).

Commands by Usage

This chapter presents access services commands alphabetically. Use Table 6 to located commands in this chapter based on their use.

Table 6 Access Commands by Usage

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Privileges</td>
<td>enable on page 86</td>
</tr>
<tr>
<td></td>
<td>set enablepass on page 87</td>
</tr>
<tr>
<td></td>
<td>disable on page 85</td>
</tr>
<tr>
<td></td>
<td>quit on page 86</td>
</tr>
</tbody>
</table>

**disable**

Changes the CLI session from enabled mode to restricted access.

**Syntax** — `disable`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command restricts access to the CLI for the current session:

```
WX1200# disable
WX1200>
```

**See Also**

- `enable` on page 86
*enable*

Places the CLI session in enabled mode, which provides access to all commands required for configuring and monitoring the system.

**Syntax** — `enable`

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Usage** — MSS displays a password prompt to challenge you with the enable password. To enable a session, your or another administrator must have configured the enable password to this WX switch with the `set enablepass` command.

**Examples** — The following command plus the enable password provides enabled access to the CLI for the current sessions:

```plaintext
WX1200> enable
Enter password: password
WX1200#
```

**See Also**

- `set enablepass` on page 87
- `set confirm` on page 105

*quit*

Exit from the CLI session.

**Syntax** — `quit`

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — To end the administrator's session, type the following command:

```plaintext
WX1200> quit
```
### set enablepass

Sets the password that provides enabled access (for configuration and monitoring) to the WX switch.

**Syntax** — `set enablepass`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — After typing the `set enablepass` command, press Enter. If you are entering the first enable password on this WX switch, press Enter at the **Enter old password** prompt. Otherwise, type the old password. Then type a password of up to 32 alphanumeric characters with no spaces, and reenter it at the **Retype new password** prompt.

> **CAUTION:** Be sure to use a password that you will remember. If you lose the enable password, the only way to restore it causes the system to return to its default settings and wipes out the configuration.

**Examples** — The following example illustrates the prompts that the system displays when the enable password is changed. The passwords you enter are not displayed.

```
WX1200# set enablepass
Enter old password: old-password
Enter new password: new-password
Retype new password: new-password
Password changed
```

**See Also**

- `disable` on page 85
- `enable` on page 86
3  

**System Service Commands**

Use system services commands to configure and monitor system information for a WX switch.

<table>
<thead>
<tr>
<th>Commands by Usage</th>
<th>Table 7: System Services Commands by Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Configuration</td>
<td>quickstart on page 100</td>
</tr>
<tr>
<td>Auto-Config</td>
<td>set auto-config on page 100</td>
</tr>
<tr>
<td>Display</td>
<td>clear banner motd on page 90</td>
</tr>
<tr>
<td></td>
<td>quickstart on page 100</td>
</tr>
<tr>
<td></td>
<td>display banner motd on page 93</td>
</tr>
<tr>
<td></td>
<td>set banner acknowledge on page 102</td>
</tr>
<tr>
<td></td>
<td>set confirm on page 105</td>
</tr>
<tr>
<td></td>
<td>set length on page 105</td>
</tr>
<tr>
<td>System Identification</td>
<td>set prompt on page 107</td>
</tr>
<tr>
<td></td>
<td>set system name on page 116</td>
</tr>
<tr>
<td></td>
<td>set system location on page 115</td>
</tr>
<tr>
<td></td>
<td>set system contact on page 108</td>
</tr>
<tr>
<td></td>
<td>set system countrycode on page 109</td>
</tr>
<tr>
<td></td>
<td>set system idle-timeout on page 113</td>
</tr>
<tr>
<td></td>
<td>set system idle-timeout on page 113</td>
</tr>
<tr>
<td></td>
<td>display load on page 95</td>
</tr>
<tr>
<td></td>
<td>display system on page 95</td>
</tr>
</tbody>
</table>
**clear banner motd** Deletes the message-of-the-day (MOTD) banner that is displayed before the login prompt for each CLI session on the wireless LAN switch.

**Syntax** — `clear banner motd`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To clear a banner, type the following command:

```
WX4400# clear banner motd
success: change accepted
```

As an alternative to clearing the banner, you can overwrite the existing banner with an empty banner by typing the following command:

```
set banner motd ^^
```

**See Also**
- `display banner motd` on page 93
- `quickstart` on page 100
clear history

Deletes the command history buffer for the current CLI session.

Syntax — clear history

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To clear the history buffer, type the following command:
WX4400# clear history
success: command buffer was flushed.

See Also
- history on page 99

clear prompt

Resets the system prompt to its previously configured value. If the prompt was not configured previously, this command resets the prompt to its default.

Syntax — clear prompt

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the prompt, type the following command:
wildebeest# clear prompt
success: change accepted.
WX4400#

See Also
- set prompt on page 107. (For information about default prompts, see “Command Prompts” on page 76.)
clear system

Clears the system configuration of the specified information.

**CAUTION:** If you change the IP address, any currently configured Mobility Domain operations cease. You must reset the Mobility Domain.

**Syntax**
```
clear system [contact | countrycode | idle-timeout | ip-address | location | name]
```

- **contact** — Resets the name of contact person for the WX switch to null.
- **countrycode** — Resets the country code for the WX switch to null.
- **idle-timeout** — Resets the number of seconds a CLI management session can remain idle to the default value (3600 seconds).
- **ip-address** — Resets the IP address of the WX switch to null.
- **location** — Resets the location of the WX switch to null.
- **name** — Resets the name of the WX switch to the default system name, which is the model number.

**Defaults** — None.

**Access** — Enabled.


**Examples** — To clear the location of the WX switch, type the following command:
```
WX4400# clear system location
success: change accepted.
```

**See Also**
- display config on page 723
- display system on page 95
- set system contact on page 108
- set system countrycode on page 109
- set system idle-timeout on page 113
- set system idle-timeout on page 113
- set system location on page 115
### display banner motd

Shows the banner that was configured with the `set banner motd` command.

**Syntax**

```plaintext
display banner motd
```

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples**

To show the banner with the message of the day, type the following command:

```plaintext
WX4400# display banner motd
hello world
```

**See Also**

- `clear banner motd` on page 90
- `quickstart` on page 100

### display base-information

Provides an in-depth snapshot of the status of the wireless LAN switch, which includes details about the boot image, the version, ports, and other configuration values. This command also displays the last 100 log messages.

**Syntax**

```plaintext
display base-information [file [subdirname/]filename]
```

- `[subdirname/]filename` — Optional subdirectory name, and a string up to 32 alphanumeric characters. The command's output is saved into a file with the specified name in nonvolatile storage.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Enter this command before calling for Technical Support. See “Obtaining Support for Your 3Com Products” on page 787 for more information.
See Also

- display boot on page 722
- display config on page 723
- display license on page 94
- display system on page 95
- display version on page 725

display license

Displays information about the license currently installed on the WX switch.

**Syntax** — display license

**Defaults** — None.

**Access** — All.

**Examples** — To view the WX switch license, type the following command:

```
WX4400# display license
Serial Number    : M8XE4IBBDB10
License Number   : 245
License Key      : WXL-076E-93E9-62DA-54D8
Activation key   : WXA-3E04-4CC2-430D-B508
Feature          : 24 additional ports
Expires          : Never
```

The additional ports refers to the number of additional MAPs the switch can boot and actively manage.

**See Also**

- set license on page 106
**display load**

Displays CPU usage on a WX switch.

**Syntax** — display load

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.1.

**Examples** — To display the CPU load recorded from the time the WX switch was booted, as well as from the previous time the display load command was run, type the following command:

```
WX4400# display load
System Load: overall: 2% delta: 5%
```

The overall field shows the CPU load as a percentage from the time the WX switch was booted. The delta field shows CPU load as a percentage from the last time the display load command was entered.

**See Also**

- display system on page 95

---

**display system**

Shows system information.

**Syntax** — display system

**Defaults** — None.

**Access** — Enabled.
Examples — To show system information, type the following command:

```
WX4400# display system
```

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
<td>Switch model number.</td>
</tr>
<tr>
<td>System Name</td>
<td>System name (factory default, or optionally configured with set system name).</td>
</tr>
<tr>
<td>System Countrycode</td>
<td>Country-specific 802.11 code required for MAP operation (configured with set system countrycode).</td>
</tr>
<tr>
<td>System Location</td>
<td>Record of the WX switch’s physical location (optionally configured with set system location).</td>
</tr>
<tr>
<td>System Contact</td>
<td>Contact information about the system administrator or another person to contact about the system (optionally configured with set system contact).</td>
</tr>
<tr>
<td>System IP</td>
<td>Common interface, source, and default IP address for the device, in dotted decimal notation (configured with set system ip-address).</td>
</tr>
</tbody>
</table>

---

Table 8 describes the fields of **display system output**.

---

Product Name: WX4400
System Name: WX-bldg3
System Countrycode: US
System Location: first-floor-bldg3
System Contact: tamara@example.com
System IP: 192.168.12.7
System idle timeout: 3600
System MAC: 00:0B:0E:00:04:30

Boot Time: 2003-11-07 15:45:49
Uptime: 13 days 04:29:10

Fan status: fan1 OK fan2 OK fan3 OK
Temperature: temp1 ok temp2 ok temp3 ok
PSU Status: Lower Power Supply DC ok AC ok  Upper Power Supply missing
Memory: 97.04/744.03 (13%)
Total Power Over Ethernet : 29.000
Table 8  display system output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System idle timeout</td>
<td>Number of seconds MSS allows a CLI management session (console, Telnet, or SSH) to remain idle before terminating the session. (The system idle timeout can be configured using the set system idle-timeout command.)</td>
</tr>
<tr>
<td>System MAC</td>
<td>WX switch’s media access control (MAC) machine address set at the factory, in 6-byte hexadecimal format.</td>
</tr>
<tr>
<td>License</td>
<td>License level installed on the WX switch (if applicable).</td>
</tr>
<tr>
<td>Boot Time</td>
<td>Date and time of the last system reboot.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Number of days, hours, minutes, and seconds that the WX has been operating since its last restart.</td>
</tr>
<tr>
<td>Fan status</td>
<td>Operating status of the WX switch’s three cooling fans:</td>
</tr>
<tr>
<td></td>
<td>- OK — Fan is operating.</td>
</tr>
<tr>
<td></td>
<td>- Failed — Fan is not operating. MSS sends an alert to the system log every 5 minutes until this condition is corrected.</td>
</tr>
<tr>
<td></td>
<td>Fan 1 is located nearest the front of the chassis, and fan 3 is located nearest the back.</td>
</tr>
<tr>
<td>Temperature</td>
<td>Status of temperature sensors at three locations in the WX switch:</td>
</tr>
<tr>
<td></td>
<td>- ok — Temperature is within the acceptable range of 0° C to 50° C (32° F to 122° F).</td>
</tr>
<tr>
<td></td>
<td>- Alarm — Temperature is above or below the acceptable range. MSS sends an alert to the system log every 5 minutes until this condition is corrected.</td>
</tr>
<tr>
<td>PSU Status</td>
<td>Status of the lower and upper power supply units:</td>
</tr>
<tr>
<td></td>
<td>- missing — Power supply is not installed or is inoperable.</td>
</tr>
<tr>
<td></td>
<td>- DC ok — Power supply is producing DC power.</td>
</tr>
<tr>
<td></td>
<td>- DC output failure — Power supply is not producing DC power. MSS sends an alert to the system log every 5 minutes until this condition is corrected.</td>
</tr>
<tr>
<td></td>
<td>- AC ok — Power supply is receiving AC power.</td>
</tr>
<tr>
<td></td>
<td>- AC not present — Power supply is not receiving AC power.</td>
</tr>
</tbody>
</table>
Help command:

Displays a list of commands that can be used to configure and monitor the WX switch.

Syntax — help

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — Use this command to see a list of available commands. If you have restricted access, you see fewer commands than if you have enabled access. To show a list of CLI commands available at the enabled access level, type the following command at the enabled access level:

WX4400# help
Commands:
-------------------------------------------------------------------------
clear Clear, use 'clear help' for more information
commit Commit the content of the ACL table
copy Copy from filename (or url) to filename (or url)
**history**

Displays the command history buffer for the current CLI session.

**Syntax** — `history`

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — To show the history of your session, type the following command:

```
WX4400> history
Display History (most recent first)
-----------------------------
[00] display config
[01] display version
[02] enable
```
See Also

- clear history on page 91

quickstart

Runs a script that interactively helps you configure a new switch.

(For more information, see the “CLI quickstart Command” section of the “WX Setup Methods” chapter in the Wireless LAN Switch and Controller Configuration Guide.)

⚠️ CAUTION: The quickstart command is for configuration of a new switch only. After prompting you for verification, the command erases the switch’s configuration before continuing. If you run this command on a switch that already has a configuration, the configuration will be erased. In addition, error messages such as “Critical AP Notice” for directly connected MAPs can appear.

set auto-config

Enables a WX switch to contact a 3WXM server for its configuration.

**Syntax** — set auto-config {enable | disable}

- enable — Enables the switch to contact a 3WXM server to request a configuration.
- disable— Disables the auto-config option.

**Defaults** — The auto-config option is automatically enabled on an unconfigured WXR100 when the factory reset switch is pressed during power on. However, auto-config is disabled by default on other models.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — A network administrator at the corporate office can preconfigure the switch in a 3WXM network plan. The switch configuration must have a name for the switch, the model must be WXR100, and the serial number must match the switch’s serial number. The configuration should also include all other settings required for the deployment, including MAP configuration, SSIDs, AAA settings, and so on.
When the 3WXM server in the corporate network receives the configuration request, the server looks in the currently open network plan for a switch configuration with the same model and serial number as the one in the configuration request.

- If the network plan contains a configuration with a matching model and serial number, 3WXM sends the configuration to the switch and restarts the switch. The switch boots using the configuration it received from 3WXM.

- If the network plan does not have a configuration with a matching model and serial number, a verification warning appears in 3WXM. The warning lists the switch’s serial number and IP address. The network administrator can upload the switch into the network plan, configure switch parameters, and deploy the configuration to the switch.

To use the auto-config option with a new (unconfigured) WXR100, insert a paperclip or similar object into the WXR100’s factory reset hole to press the switch. The factory reset switch must be held for about 3 seconds while the factory reset LED (the right LED above port 1) is lit. Normally, this LED remains solidly lit for 3 seconds after power on. However, when the factory reset switch is pressed, the LED flashes for 3 seconds instead.

If you want another WX switch model to be able to access a 3WXM server for a configuration, you also must preconfigure the WX with the following information:

- IP address
- Gateway address
- Domain name and DNS server address

You can enable the switch to use the MSS DHCP client to obtain this information from a DHCP server in the local network where the switch will be deployed. Alternatively, you can statically configure the information.

The IP address and DNS information are configured independently. You can configure the combination of settings that work with the network resources available at the deployment site. The following examples show some of the combinations you can configure.
Examples — The following commands stage a WX switch to use the auto-config option. The network where the switch is installed has a DHCP server, so the switch is configured to use the MSS DHCP client to obtain an IP address, default gateway address, DNS domain name, and DNS server IP addresses:

1 Configure a VLAN:

   WX-1200# set vlan 1 port 7
   success: change accepted.

2 Enable the DHCP client on VLAN 1:

   WX-1200# set interface 1 ip dhcp-client enable
   success: change accepted.

3 Enable the auto-config option:

   WX-1200# set auto-config enable
   success: change accepted.

4 Save the configuration changes:

   WX-1200# save config
   success: configuration saved.

See Also

- crypto generate key on page 613
- crypto generate self-signed on page 616
- save config on page 733
- set interface dhcp-client on page 219
- set vlan port on page 173

set banner acknowledge

Configures a prompt that is displayed following the MOTD banner. The user must acknowledge the prompt in order to gain access to the system.

Syntax — set banner acknowledge mode {enable | disable}

Syntax — set banner acknowledge message “message”

- enable — Enables the prompt to acknowledge the MOTD banner.
- disable — Disables the prompt to acknowledge the MOTD banner.
- “ — Delimiting character that begins and ends the prompt message; for example, double quotes (").
- **message** — Up to 32 alphanumeric characters, but **not** the delimiting character.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** Enable the MOTD prompt, then optionally specify a prompt message.

When a user logs into the WX switch using the CLI, the configured MOTD banner is displayed, followed by the MOTD prompt message (if one is specified). In response, the user has the option of entering `y` to proceed or any other key to terminate the connection.

**Examples** — To enable the prompt for the MOTD banner, type the following command:

```
WX# set banner acknowledge enable
success: change accepted.
```

To set *Do you agree?* as the text to be displayed following the MOTD banner, type the following command:

```
WX# set banner acknowledge message "Do you agree?"
success: change accepted.
```

After these commands are entered, when the user logs on, the MOTD banner is displayed, followed by the text *Do you agree?* If the user enters `y`, then the login proceeds; if not, then the user is disconnected.

**See Also**

- [set banner motd](#) on page 104
- [clear banner motd](#) on page 90
- [display banner motd](#) on page 93
set banner motd

Configures the banner string that is displayed before the beginning of each login prompt for each CLI session on the WX switch.

Syntax — set banner motd "text"

- " — Delimiting character that begins and ends the message; for example, double quotes (".
- text — Up to 2000 alphanumeric characters, including tabs and carriage returns, but not the delimiting character (^). The maximum number of characters is approximately 24 lines by 80 characters.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Type a delimiting character, then the message, then another delimiting character.

Examples — To create a banner that says Meeting @ 4:00 p.m. in Conference Room #3, type the following command:

WX# set banner motd "Meeting @ 4:00 p.m. in Conference Room #3"
success: motd changed.

See Also
- set banner acknowledge on page 102
- clear banner motd on page 90
- display banner motd on page 93
**set confirm**

Enables or disables the display of confirmation messages for commands that might have a large impact on the network.

**Syntax** — `set confirm {on | off}`

- **on** — Enables confirmation messages.
- **off** — Disables confirmation messages.

**Defaults** — Configuration messages are enabled.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command remains in effect for the duration of the session, until you enter a `quit` command, or until you enter another `set confirm` command.

MSS displays a message requiring confirmation when you enter certain commands that can have a potentially large impact on the network. For example:

```
WX4400# clear vlan red
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]
```

**Examples** — To turn off these confirmation messages, type the following command:

```
WX4400# set confirm off
success: Confirm state is off
```

**set length**

Defines the number of lines of CLI output to display between paging prompts. MSS displays the set number of lines and waits for you to press any key to display another set, or type `q` to quit the display.

**Syntax** — `set length number-of-lines`

- **number-of-lines** — Number of lines of text to display between paging prompts. You can specify from 0 to 512. The 0 value disables the paging prompt action entirely.

**Defaults** — MSS displays 24 lines by default.

**Access** — All.
**CHAPTER 3: SYSTEM SERVICE COMMANDS**

**History** — Introduced in MSS Version 3.0.

**Usage** — Use this command if the output of a CLI command is greater than the number of lines allowed by default for a terminal type.

**Examples** — To set the number of lines displayed to 100, type the following command:

```
WX4400# set length 100
success: screen length for this session set to 100
```

---

**set license**

Installs an upgrade license, for managing more MAPs.

**Syntax** — `set license license-key activation-key`

- `license-key` — License key, starting with WXL. You can enter the key with or without the hyphens.
- `activation-key` — Activation key, starting with WXA. You can enter the key with or without the hyphens.

**Defaults** — The WX4400 can boot and manage 24 MAPs by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — The license key is shipped with the switch. To obtain the activation key, access the 3Com web site. Each license and activation key pair allows the switch to actively manage an additional 24 MAPs. You can install up to three upgrade license and activation key pairs, to actively manage up to 96 MAPs.

**Examples** — To install an upgrade license and activation key, type the following command:

```
WX4400# set license WXL-076E-93E9-62DA-54D8
WXA-3E04-4CC2-430D-B508
Serial Number    : M8XE41BB8DB10
License Number   : 245
License Key      : WXL-076E-93E9-62DA-54D8
Activation key   : WXA-3E04-4CC2-430D-B508
Feature          : 24 additional ports
Expires          : Never
```
set prompt

Changes the CLI prompt for the WX switch to a string you specify.

**Syntax** — *set prompt string*

- **string** — Alphanumeric string up to 32 characters long. To include spaces in the prompt, you must enclose the string in double quotation marks ("").

**Defaults** — The factory default for the WX switch name is the model number (*WX1200* for the 3Com Wireless LAN Switch WX1200, *WX4400* for the 3Com Wireless LAN Controller WX4400).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — When you first log in for the initial configuration of the WX switch, the CLI provides a *WX1200>* or *WX4400>* prompt, depending on your model. After you become enabled by typing *enable* and giving a suitable password, the *WX1200#* or *WX4400#* prompt is displayed.

If you use the *set system name* command to change the default system name, MSS uses that name in the prompt, unless you also change the prompt with *set prompt*.

**Examples** — The following example sets the prompt from *WX4400* to *happy_days*:

```
WX4400# set prompt happy_days
success: change accepted.
happy_days#
```

**See Also**

- *clear prompt* on page 91
set system contact Stores a contact name for the WX switch.

**Syntax** — set system contact string

- **string** — Alphanumeric string up to 256 characters long, with no blank spaces.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

To view the system contact string, type the `display system` command.

**Examples** — The following command sets the system contact information to tamara@example.com:

WX1200# set system contact tamara@example.com
success: change accepted.

**See Also**

- clear system on page 92
- display system on page 95
- set system location on page 115
- set system name on page 116
set system countrycode

Defines the country-specific IEEE 802.11 regulations to enforce on the WX switch.

Syntax — set system countrycode code

- code — Two-letter code for the country of operation for the WX switch. You can specify one of the codes listed in Table 9.

Table 9  Country Codes

<table>
<thead>
<tr>
<th>Country</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algeria</td>
<td>DZ</td>
</tr>
<tr>
<td>Argentina</td>
<td>AR</td>
</tr>
<tr>
<td>Australia</td>
<td>AU</td>
</tr>
<tr>
<td>Austria</td>
<td>AT</td>
</tr>
<tr>
<td>Bahrain</td>
<td>BH</td>
</tr>
<tr>
<td>Belgium</td>
<td>BE</td>
</tr>
<tr>
<td>Belize</td>
<td>BZ</td>
</tr>
<tr>
<td>Bolivia</td>
<td>BO</td>
</tr>
<tr>
<td>Bozna and Herzegovina</td>
<td>BA</td>
</tr>
<tr>
<td>Brazil</td>
<td>BR</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>BG</td>
</tr>
<tr>
<td>Canada</td>
<td>CA</td>
</tr>
<tr>
<td>Chile</td>
<td>CL</td>
</tr>
<tr>
<td>China</td>
<td>CN</td>
</tr>
<tr>
<td>Colombia</td>
<td>CO</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>CR</td>
</tr>
<tr>
<td>Cote d’Ivoire</td>
<td>CI</td>
</tr>
<tr>
<td>Croatia</td>
<td>HR</td>
</tr>
<tr>
<td>Cyprus</td>
<td>CY</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>CZ</td>
</tr>
<tr>
<td>Denmark</td>
<td>DK</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>DO</td>
</tr>
<tr>
<td>Ecuador</td>
<td>EC</td>
</tr>
<tr>
<td>El Salvador</td>
<td>SV</td>
</tr>
</tbody>
</table>

(continued)
<table>
<thead>
<tr>
<th>Country</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egypt</td>
<td>EG</td>
</tr>
<tr>
<td>Estonia</td>
<td>EE</td>
</tr>
<tr>
<td>Finland</td>
<td>FI</td>
</tr>
<tr>
<td>France</td>
<td>FR</td>
</tr>
<tr>
<td>Germany</td>
<td>DE</td>
</tr>
<tr>
<td>Greece</td>
<td>GR</td>
</tr>
<tr>
<td>Guatemala</td>
<td>GT</td>
</tr>
<tr>
<td>Honduras</td>
<td>HN</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>HK</td>
</tr>
<tr>
<td>Hungary</td>
<td>HU</td>
</tr>
<tr>
<td>Iceland</td>
<td>IS</td>
</tr>
<tr>
<td>India</td>
<td>IN</td>
</tr>
<tr>
<td>Indonesia</td>
<td>ID</td>
</tr>
<tr>
<td>Ireland</td>
<td>IE</td>
</tr>
<tr>
<td>Israel</td>
<td>IL</td>
</tr>
<tr>
<td>Italy</td>
<td>IT</td>
</tr>
<tr>
<td>Jamaica</td>
<td>JM</td>
</tr>
<tr>
<td>Japan</td>
<td>JP</td>
</tr>
<tr>
<td>Jordan</td>
<td>JO</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>KZ</td>
</tr>
<tr>
<td>Kenya</td>
<td>KE</td>
</tr>
<tr>
<td>Kuwait</td>
<td>KW</td>
</tr>
<tr>
<td>Latvia</td>
<td>LV</td>
</tr>
<tr>
<td>Lebanon</td>
<td>LB</td>
</tr>
<tr>
<td>Liechtenstein</td>
<td>LI</td>
</tr>
<tr>
<td>Lithuania</td>
<td>LT</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>LU</td>
</tr>
<tr>
<td>Macedonia, former Yugoslav Republic of</td>
<td>MK</td>
</tr>
<tr>
<td>Malaysia</td>
<td>MY</td>
</tr>
<tr>
<td>Malta</td>
<td>MT</td>
</tr>
<tr>
<td>Mauritius</td>
<td>MU</td>
</tr>
</tbody>
</table>

(continued)
<table>
<thead>
<tr>
<th>Country</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mexico</td>
<td>MX</td>
</tr>
<tr>
<td>Morocco</td>
<td>MA</td>
</tr>
<tr>
<td>Namibia</td>
<td>NA</td>
</tr>
<tr>
<td>Netherlands</td>
<td>NL</td>
</tr>
<tr>
<td>New Zealand</td>
<td>NZ</td>
</tr>
<tr>
<td>Nigeria</td>
<td>NG</td>
</tr>
<tr>
<td>Norway</td>
<td>NO</td>
</tr>
<tr>
<td>Oman</td>
<td>OM</td>
</tr>
<tr>
<td>Pakistan</td>
<td>PK</td>
</tr>
<tr>
<td>Panama</td>
<td>PA</td>
</tr>
<tr>
<td>Paraguay</td>
<td>PY</td>
</tr>
<tr>
<td>Peru</td>
<td>PE</td>
</tr>
<tr>
<td>Philippines</td>
<td>PH</td>
</tr>
<tr>
<td>Poland</td>
<td>PL</td>
</tr>
<tr>
<td>Portugal</td>
<td>PT</td>
</tr>
<tr>
<td>Puerto Rico</td>
<td>PR</td>
</tr>
<tr>
<td>Qatar</td>
<td>QA</td>
</tr>
<tr>
<td>Romania</td>
<td>RO</td>
</tr>
<tr>
<td>Russia</td>
<td>RU</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>SA</td>
</tr>
<tr>
<td>Serbia</td>
<td>CS</td>
</tr>
<tr>
<td>Singapore</td>
<td>SG</td>
</tr>
<tr>
<td>Slovakia</td>
<td>SK</td>
</tr>
<tr>
<td>Slovenia</td>
<td>SI</td>
</tr>
<tr>
<td>South Africa</td>
<td>ZA</td>
</tr>
<tr>
<td>South Korea</td>
<td>KR</td>
</tr>
<tr>
<td>Spain</td>
<td>ES</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>LK</td>
</tr>
<tr>
<td>Sweden</td>
<td>SE</td>
</tr>
<tr>
<td>Switzerland</td>
<td>CH</td>
</tr>
<tr>
<td>Taiwan</td>
<td>TW</td>
</tr>
<tr>
<td>Thailand</td>
<td>TH</td>
</tr>
</tbody>
</table>

(continued)
Defaults — The factory default country code is None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must set the system county code to a valid value before using any set ap commands to configure a MAP.

Examples — To set the country code to Canada, type the following command:

```plaintext
WX1200# set system country code CA
success: change accepted.
```

See Also

* display config on page 723

---

Table 9  Country Codes (continued)

<table>
<thead>
<tr>
<th>Country</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trinidad and Tobago</td>
<td>TT</td>
</tr>
<tr>
<td>Tunisia</td>
<td>TN</td>
</tr>
<tr>
<td>Turkey</td>
<td>TR</td>
</tr>
<tr>
<td>Ukraine</td>
<td>UA</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>AE</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>GB</td>
</tr>
<tr>
<td>United States</td>
<td>US</td>
</tr>
<tr>
<td>Uruguay</td>
<td>UY</td>
</tr>
<tr>
<td>Venezuela</td>
<td>VE</td>
</tr>
<tr>
<td>Vietnam</td>
<td>VN</td>
</tr>
</tbody>
</table>
**set system idle-timeout**  

Specifies the maximum number of seconds a CLI management session with the switch can remain idle before MSS terminates the session.

**Syntax** — set system idle-timeout seconds

- **seconds** — Number of seconds a CLI management session can remain idle before MSS terminates the session. You can specify from 0 to 86400 seconds (one day). If you specify 0, the idle timeout is disabled.

  The timeout interval is in 30-second increments. For example, the interval can be 0, or 30 seconds, or 60 seconds, or 90 seconds, and so on. If you enter an interval that is not divisible by 30, the CLI rounds up to the next 30-second increment. For example, if you enter 31, the CLI rounds up to 60.

**Defaults** — 3600 seconds (one hour).

**Access** — Enabled.

**History** — Introduced in MSS Version 4.1.

**Usage** — This command applies to all types of CLI management sessions: console, Telnet, and SSH. The timeout change applies to existing sessions only, not to new sessions.

**Examples** — The following command sets the idle timeout to 1800 seconds (one half hour):

```
WX1200# set system idle-timeout 1800
success: change accepted.
```

**See Also**

- clear system on page 92
- display system on page 95
set system ip-address

Sets the system IP address so that it can be used by various services in the WX switch.

⚠️ **CAUTION:** Any currently configured Mobility Domain operations cease if you change the IP address. If you change the address, you must reset the Mobility Domain.

**Syntax** — `set system ip-address ip-addr`
- `ip-addr` — IP address, in dotted decimal notation.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command sets the IP address of the WX switch to 192.168.253.1:

```
WX4400# set system ip-address 192.168.253.1
success: change accepted.
```

**See Also**
- `clear system` on page 92
- `set interface` on page 218
- `display system` on page 95
**set system location**

Stores location information for the WX switch.

**Syntax** — `set system location string`

- `string` — Alphanumeric string up to 256 characters long, with no blank spaces.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You cannot include spaces in the system location string.

To view the system location string, type the `display system` command.

**Examples** — To store the location of the WX switch in the WX’s configuration, type the following command:

```
WX4400# set system location first-floor-bldg3
success: change accepted.
```

**See Also**

- `clear system` on page 92
- `display system` on page 95
- `set system contact` on page 108
- `set system name` on page 116
set system name

Changes the name of the WX switch from the default system name and also provides content for the CLI prompt, if you do not specify a prompt.

**Syntax** — set system name string

- **string** — Alphanumeric string up to 256 characters long, with no blank spaces. Use a unique name for each WX switch.

**Defaults** — By default, the system name and command prompt have the same value. The factory default for both is the model number (WX1200 for the 3Com Wireless LAN Switch WX1200, WX4400 for the 3Com Wireless LAN Controller WX4400).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Entering set system name with no string resets the system name to the factory default.

To view the system name string, type the display system command.

**Examples** — The following example sets the system name to a name that identifies the WX switch:

WX4400# set system name WX-bldg3
success: change accepted.
WX-bldg3#

**See Also**
- clear system on page 92
- display system on page 95
- set prompt on page 107
- set system contact on page 108
- set system location on page 115
Use port commands to configure and manage individual ports and load-sharing port groups.

This chapter presents port commands alphabetically. Use Table 10 to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Commands by Usage</th>
<th>Table 10 Port Commands by Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>Port Type</td>
<td>set port type ap on page 145</td>
</tr>
<tr>
<td></td>
<td>set ap on page 135</td>
</tr>
<tr>
<td></td>
<td>set port type wired-auth on page 148</td>
</tr>
<tr>
<td></td>
<td>clear port type on page 122</td>
</tr>
<tr>
<td></td>
<td>clear ap on page 118</td>
</tr>
<tr>
<td>Name</td>
<td>set port name on page 141</td>
</tr>
<tr>
<td></td>
<td>clear port name on page 120</td>
</tr>
<tr>
<td>State</td>
<td>set port on page 137</td>
</tr>
<tr>
<td></td>
<td>reset port on page 135</td>
</tr>
<tr>
<td></td>
<td>display port status on page 127</td>
</tr>
<tr>
<td>Gigabit Interface Type</td>
<td>display port media-type on page 129</td>
</tr>
<tr>
<td></td>
<td>set port media-type on page 139</td>
</tr>
<tr>
<td></td>
<td>clear port media-type on page 120</td>
</tr>
<tr>
<td>Speed</td>
<td>set port speed on page 143</td>
</tr>
<tr>
<td>Autonegotiation</td>
<td>set port negotiation on page 141</td>
</tr>
<tr>
<td>PoE</td>
<td>set port poe on page 142</td>
</tr>
<tr>
<td>SNMP</td>
<td>set port trap on page 144</td>
</tr>
</tbody>
</table>
Table 10  Port Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Groups</td>
<td>set port-group on page 138</td>
</tr>
<tr>
<td></td>
<td>display port-group on page 124</td>
</tr>
<tr>
<td></td>
<td>clear port-group on page 119</td>
</tr>
<tr>
<td>Port Mirroring</td>
<td>display port mirror on page 125</td>
</tr>
<tr>
<td></td>
<td>clear port mirror on page 121</td>
</tr>
<tr>
<td></td>
<td>set port mirror on page 140</td>
</tr>
<tr>
<td>Statistics</td>
<td>display port counters on page 123</td>
</tr>
<tr>
<td></td>
<td>monitor port counters on page 130</td>
</tr>
<tr>
<td></td>
<td>clear port counters on page 119</td>
</tr>
</tbody>
</table>

**clear ap**  
Removes a Distributed MAP.

⚠️ **CAUTION:** When you clear a Distributed MAP, MSS ends user sessions that are using the MAP.

**Syntax** — `clear ap {ap-number | all}
- `ap-number` — Number of the Distributed MAP(s) to remove.
- `all` — Clear all distributed MAPs.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 6.0 renamed `dap` to `ap`.

**Examples** — The following command clears Distributed MAP 1:

```
WX4400# clear ap 1
This will clear specified AP devices.
Would you like to continue? (y/n) [n] y
```

**See Also**
- `set ap` on page 135
- `set port type ap` on page 145
**clear port counters**

Clears port statistics counters and resets them to 0.

**Syntax** — `clear port counters`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command clears all port statistics counters and resets them to 0:

```
WX4400# clear port counters
success: cleared port counters
```

**See Also**
- `display port counters` on page 123
- `monitor port counters` on page 130

**clear port-group**

Removes a port group.

**Syntax** — `clear port-group name name`

- `name name` — Name of the port group.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command clears port group server1:

```
WX4400# clear port-group name server1
success: change accepted.
```

**See Also**
- `set port-group` on page 138
- `display port-group` on page 124
### clear port media-type

Disables the copper interface and reenables the fiber interface on an WX4400 gigabit Ethernet port.

**Syntax** — `clear port media-type port-list`

- `port-list` — List of physical ports. MSS disables the copper interface and reenables the fiber interface on all the specified ports.

**Defaults** — The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — This command applies only to the WX4400. This command does not affect a link that is already active on the port.

**Examples** — The following command disables the copper interface and reenables the fiber interface on port 2:

```
WX4400# clear port media-type 2
```

**See Also**
- `set port media-type` on page 139
- `display port media-type` on page 129

### clear port name

Removes the name assigned to a port.

**Syntax** — `clear port port-list name`

- `port-list` — List of physical ports. MSS removes the names from all the specified ports.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
clear port mirror

Examples — The following command clears the names of ports 1 through 3:

WX4400# clear port 1-3 name

See Also
• display port status on page 127
• set port name on page 141

clear port mirror

Removes a port mirroring configuration.

Syntax — clear port mirror

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Examples — The following command clears the port mirroring configuration from the switch:

WX4400# clear port mirror

See Also
• display port mirror on page 125
• set port mirror on page 140

clear port preference

Resets a gigabit Ethernet port on a WX4400 to use the GBIC (fiber) interface for the active link.

Syntax — clear port preference port-list

• port-list — List of physical ports. MSS clears the preference on all the specified ports.

Defaults — When both the copper and fiber interfaces of a gigabit Ethernet port are connected, the GBIC (fiber) interface is the active link. The RJ-45 (copper) link is unused.

Access — Enabled.
History — Introduced in MSS Version 3.0.

Usage — This command applies only to the WX4400. This command does not affect a link that is already active on the port.

Examples — The following command clears the preference set on port 2 on a WX4400 switch:

WX4400# clear port preference 2

See Also

- display port status on page 127

---

**clear port type**

Removes all configuration settings from a port and resets the port as a network port.

⚠️ **CAUTION:** When you clear a port, MSS ends user sessions that are using the port.

**Syntax** — `clear port type port-list`

- **port-list** — List of physical ports. MSS resets and removes the configuration from all the specified ports.

**Defaults** — The cleared port becomes a network port but is not placed in any VLANs.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Use this command to change a port back to a network port. All configuration settings specific to the port type are removed. For example, if you clear a MAP access point port, all MAP-specific settings are removed. Table 11 lists the default network port settings that MSS applies when you clear a port’s type.
display port counters

Table 11  Network port defaults

<table>
<thead>
<tr>
<th>Port Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN membership</td>
<td>None.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Although the command changes a port to a network port, the command does not place the port in any VLAN. To use the port in a VLAN, you must add the port to the VLAN.</td>
</tr>
<tr>
<td>Spanning Tree Protocol (STP)</td>
<td>Based on the VLAN(s) you add the port to.</td>
</tr>
<tr>
<td>802.1X</td>
<td>No authorization.</td>
</tr>
<tr>
<td>Port groups</td>
<td>None.</td>
</tr>
<tr>
<td>Internet Group Management Protocol (IGMP) snooping</td>
<td>Enabled as port is added to VLANs.</td>
</tr>
<tr>
<td>Access point and radio parameters</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Maximum user sessions</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

Examples — The following command clears port 5:

WX1200# clear port type 5
This may disrupt currently authenticated users.
Are you sure? [y/n] [n]y
success: change accepted.

See Also

- set port type ap on page 145
- set port type wired-auth on page 148

display port counters

Displays port statistics.

Syntax — display port counters

{octets | packets | receive-errors | transmit-errors | collisions | receive-etherstats | transmit-etherstats} [port port-list]

- **octets** — Shows octet statistics.
- **packets** — Shows packet statistics.
- **receive-errors** — Shows errors in received packets.
- **transmit-errors** — Shows errors in transmitted packets.
- **collisions** — Shows collision statistics.
CHAPTER 4: PORT COMMANDS

- **receive-etherstats** — Shows Ethernet statistics for received packets.
- **transmit-etherstats** — Shows Ethernet statistics for transmitted packets.
- **port port-list** — List of physical ports. If you do not specify a port list, MSS shows statistics for all ports.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can specify one statistic type with the command.

**Examples** — The following command shows octet statistics for port 3:

```
WX1200> display port counters octets port 3
Port   Status Rx Octets Tx Octets
=============================================================================  
3 Up    27965420 34886544
```

This command's output has the same fields as the **monitor port counters** command. For descriptions of the fields, see Table 17 on page 132.

**See Also**

- **clear port counters** on page 119
- **monitor port counters** on page 130

**display port-group** Shows port group information.

**Syntax** — `display port-group [name group-name]`

- **name group-name** — Shows information for the specified port group.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0. In Version 4.2 the option all was removed for simplicity. You can display information for all groups by entering the command without specifying a group name.
**Examples** — The following command displays the configuration of port group server2:

WX1200# `display port-group name server2`
Port group: server2 is up
  Ports: 5, 7

Table 12 describes the fields in the display port-group output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port group</td>
<td>Name and state (enabled or disabled) of the port group.</td>
</tr>
<tr>
<td>Ports</td>
<td>Ports contained in the port group.</td>
</tr>
</tbody>
</table>

**See Also**
- `clear port-group` on page 119
- `set port-group` on page 138

---

**display port mirror** Displays the port mirroring configuration.

**Syntax** — `display port mirror`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Examples** — The following command displays the port mirroring configuration on the switch:

WX4400# `display port mirror`
Port 1 is mirrored to port 2

If port mirroring is not configured, the message in the following example is displayed instead:

WX4400# `display port mirror`
No ports are mirrored
display port poe

Displays status information for ports on which Power over Ethernet (PoE) is enabled.

**Syntax** — `display port poe [port-list]`

- **port-list** — List of physical ports. If you do not specify a port list, PoE information is displayed for all ports.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays PoE information for all ports on a WX1200 switch:

```
WX1200# display port poe
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Link</th>
<th>Status</th>
<th>PoE Type</th>
<th>PoE config</th>
<th>Draw</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>up</td>
<td>-</td>
<td>disabled</td>
<td>off</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>down</td>
<td>-</td>
<td>disabled</td>
<td></td>
<td>off</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>down</td>
<td>-</td>
<td>disabled</td>
<td>off</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>down</td>
<td>MAP</td>
<td>enabled</td>
<td>1.44</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>down</td>
<td>-</td>
<td>disabled</td>
<td>off</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>down</td>
<td>-</td>
<td>disabled</td>
<td>off</td>
<td></td>
</tr>
</tbody>
</table>

Table 13 describes the fields in this display.

**Table 13** Output for display port poe

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number.</td>
</tr>
<tr>
<td>Name</td>
<td>Port name. If the port does not have a name, the port number is listed.</td>
</tr>
</tbody>
</table>
display port status

Table 13  Output for display port poe (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link status</td>
<td>Link status of the port:</td>
</tr>
<tr>
<td></td>
<td>- <strong>up</strong>—The port is connected.</td>
</tr>
<tr>
<td></td>
<td>- <strong>down</strong>—The port is not connected.</td>
</tr>
<tr>
<td>Port type</td>
<td>Port type:</td>
</tr>
<tr>
<td></td>
<td>- <strong>MAP</strong>—The port is a MAP access port.</td>
</tr>
<tr>
<td></td>
<td>- <strong>-</strong>—(The port is not a MAP access port.)</td>
</tr>
<tr>
<td>PoE config</td>
<td>PoE state:</td>
</tr>
<tr>
<td></td>
<td>- <strong>enabled</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>disabled</strong></td>
</tr>
<tr>
<td>PoE Draw</td>
<td>Power draw on the port, in watts.</td>
</tr>
<tr>
<td></td>
<td>For 10/100 Ethernet ports on which PoE is disabled, this field displays <strong>off</strong>. For gigabit Ethernet ports, this field displays <strong>invalid</strong>, because PoE is not supported on gigabit Ethernet ports. The value <strong>overcurrent</strong> indicates a PoE problem such as a short in the cable.</td>
</tr>
</tbody>
</table>

See Also

- **set port poe** on page 142

**display port status**

Displays configuration and status information for ports.

**Syntax** — `display port status [port-list]`

- **port-list** — List of physical ports. If you do not specify a port list, information is displayed for all ports.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.
**Examples** — The following command displays information for all ports on a WX1200 switch:

```
WX1200# display port status
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Admin</th>
<th>Oper</th>
<th>Config</th>
<th>Actual</th>
<th>Type</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>up</td>
<td>up</td>
<td>auto</td>
<td>100/full</td>
<td>network</td>
<td>10/100BaseTx</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>up</td>
<td>up</td>
<td>auto</td>
<td>100/full</td>
<td>ap</td>
<td>10/100BaseTx</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>up</td>
<td>up</td>
<td>auto</td>
<td>100/full</td>
<td>network</td>
<td>10/100BaseTx</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>up</td>
<td>down</td>
<td>auto</td>
<td>network</td>
<td>10/100BaseTx</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>up</td>
<td>down</td>
<td>auto</td>
<td>network</td>
<td>10/100BaseTx</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>up</td>
<td>down</td>
<td>auto</td>
<td>network</td>
<td>10/100BaseTx</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>up</td>
<td>down</td>
<td>auto</td>
<td>network</td>
<td>10/100BaseTx</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>up</td>
<td>down</td>
<td>auto</td>
<td>network</td>
<td>10/100BaseTx</td>
<td></td>
</tr>
</tbody>
</table>

Table 14 describes the fields in this display.

**Table 14** Output for display port status

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number.</td>
</tr>
<tr>
<td>Name</td>
<td>Port name. If the port does not have a name, the port number is listed.</td>
</tr>
<tr>
<td>Admin</td>
<td>Administrative status of the port:</td>
</tr>
<tr>
<td>Oper</td>
<td>Operational status of the port:</td>
</tr>
<tr>
<td>Config</td>
<td>Port speed configured on the port:</td>
</tr>
<tr>
<td>Actual</td>
<td>Speed and operating mode in effect on the port.</td>
</tr>
<tr>
<td>Type</td>
<td>Port type:</td>
</tr>
</tbody>
</table>

- **up** — The port is enabled.
- **down** — The port is disabled.
- **up** — The port is operational.
- **down** — The port is not operational.
- **10** — 10 Mbps.
- **100** — 100 Mbps.
- **1000** — 1000 Mbps.
- **auto** — The port sets its own speed.
- **ap** — MAP access point port
- **network** — Network port
- **wa** — Wired authentication port
display port media-type

Displays the enabled interface types on a WX4400 switch's gigabit Ethernet ports.

See Also — display port media-type [port-list]

port-list — List of physical ports. MSS displays the enabled interface types for all the specified ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 4.0.

Usage — This command applies only to the WX4400.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>Link type:</td>
</tr>
<tr>
<td>10/100BaseTX</td>
<td>10/100BASE-T.</td>
</tr>
<tr>
<td>GBIC</td>
<td>1000BASE-SX or 1000BASE-LX GBIC.</td>
</tr>
<tr>
<td>1000BaseT</td>
<td>1000BASE-T.</td>
</tr>
<tr>
<td>No connector</td>
<td>GBIC slot is empty.</td>
</tr>
</tbody>
</table>

Table 14  Output for display port status (continued)
Examples — The following command displays the enabled interface types on all four ports of a WX4400 switch:

WX4400# display port media-type

<table>
<thead>
<tr>
<th>Port</th>
<th>Media Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>GBIC</td>
</tr>
<tr>
<td>2</td>
<td>RJ45</td>
</tr>
<tr>
<td>3</td>
<td>GBIC</td>
</tr>
<tr>
<td>4</td>
<td>GBIC</td>
</tr>
</tbody>
</table>

Table 15 describes the fields in this display.

Table 15  Output for display port media-type

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number.</td>
</tr>
<tr>
<td>Preference</td>
<td>Preference setting:</td>
</tr>
<tr>
<td></td>
<td>GBIC—The GBIC (fiber) interface is enabled.</td>
</tr>
<tr>
<td></td>
<td>RJ45—The RJ-45 (copper) interface is enabled.</td>
</tr>
</tbody>
</table>

See Also

- clear port media-type on page 120
- set port media-type on page 139

**monitor port counters**

Displays and continually updates port statistics.

**Syntax** — monitor port counters
[octets | packets | receive-errors | transmit-errors | collisions | receive-etherstats | transmit-etherstats]  

- octets — Displays octet statistics first.
- packets — Displays packet statistics first.
- receive-errors — Displays errors in received packets first.
- transmit-errors — Displays errors in transmitted packets first.
- collisions — Displays collision statistics first.
- receive-etherstats — Displays Ethernet statistics for received packets first.
- **transmit-etherstats** — Displays Ethernet statistics for transmitted packets first.

**Defaults** — All types of statistics are displayed for all ports. MSS refreshes the statistics every 5 seconds. This interval cannot be configured. Statistics types are displayed in the following order by default:

- Octets
- Packets
- Receive errors
- Transmit errors
- Collisions
- Receive Ethernet statistics
- Transmit Ethernet statistics

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Usage** — Each type of statistic is displayed separately. Press the Spacebar to cycle through the displays for each type.

If you use an option to specify a statistic type, the display begins with that statistic type. You can use one statistic option with the command.

Use the keys listed in Table 16 to control the monitor display.

**Table 16**  Key Controls for Monitor Port Counters Display

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spacebar</td>
<td>Advances to the next statistic type.</td>
</tr>
<tr>
<td>Esc</td>
<td>Exits the monitor. MSS stops displaying the statistics and displays a new command prompt.</td>
</tr>
<tr>
<td>c</td>
<td>Clears the statistics counters for the currently displayed statistics type. The counters begin incrementing again.</td>
</tr>
</tbody>
</table>
For error reporting, the cyclic redundancy check (CRC) errors include misalignment errors. Jumbo packets with valid CRCs are not counted. A short packet can be reported as a short packet, a CRC error, or an overrun. In some circumstances, the transmitted octets counter might increment a small amount for a port with nothing attached.

**Examples** — The following command starts the port statistics monitor beginning with octet statistics (the default):

```
WX4400# monitor port counters
```

As soon as you press Enter, MSS clears the window and displays statistics at the top of the window.

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Rx Octets</th>
<th>Tx Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Up</td>
<td>27965420</td>
<td>34886544</td>
</tr>
</tbody>
</table>

To cycle the display to the next set of statistics, press the Spacebar. In this example, packet statistics are displayed next:

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Rx Unicast</th>
<th>Rx NonUnicast</th>
<th>Tx Unicast</th>
<th>Tx NonUnicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Up</td>
<td>54620</td>
<td>62144</td>
<td>68318</td>
<td>62556</td>
</tr>
</tbody>
</table>

Table 17 describes the port statistics displayed by each statistics option. The Port and Status fields are displayed for each option.

**Table 17** Output for monitor port counters

<table>
<thead>
<tr>
<th>Statistics Option</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displayed for All Options octets</td>
<td>Port</td>
<td>Port the statistics are displayed for.</td>
</tr>
<tr>
<td></td>
<td>Status</td>
<td>Port status. The status can be Up or Down.</td>
</tr>
<tr>
<td></td>
<td>Rx Octets</td>
<td>Total number of octets received by the port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This number includes octets received in frames that contained errors.</td>
</tr>
<tr>
<td></td>
<td>Tx Octets</td>
<td>Total number of octets received.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This number includes octets received in frames that contained errors.</td>
</tr>
</tbody>
</table>
Table 17  Output for monitor port counters (continued)

<table>
<thead>
<tr>
<th>Statistics Option</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
<td>Rx Unicast</td>
<td>Number of unicast packets received. This number does not include packets that contain errors.</td>
</tr>
<tr>
<td></td>
<td>Rx NonUnicast</td>
<td>Number of broadcast and multicast packets received. This number does not include packets that contain errors.</td>
</tr>
<tr>
<td></td>
<td>Tx Unicast</td>
<td>Number of unicast packets transmitted. This number does not include packets that contain errors.</td>
</tr>
<tr>
<td></td>
<td>Tx NonUnicast</td>
<td>Number of broadcast and multicast packets transmitted. This number does not include packets that contain errors.</td>
</tr>
<tr>
<td>receive-errors</td>
<td>Rx Crc</td>
<td>Number of frames received by the port that had the correct length but contained an invalid frame check sequence (FCS) value. This statistic includes frames with misalignment errors.</td>
</tr>
<tr>
<td></td>
<td>Rx Error</td>
<td>Total number of frames received in which the Physical layer (PHY) detected an error.</td>
</tr>
<tr>
<td></td>
<td>Rx Short</td>
<td>Number of frames received by the port that were fewer than 64 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Rx Overrun</td>
<td>Number of frames received by the port that were valid but were longer than 1518 bytes. This statistic does not include jumbo packets with valid CRCs.</td>
</tr>
<tr>
<td>transmit-errors</td>
<td>Tx Crc</td>
<td>Number of frames transmitted by the port that had the correct length but contained an invalid FCS value.</td>
</tr>
<tr>
<td></td>
<td>Tx Short</td>
<td>Number of frames transmitted by the port that were fewer than 64 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Tx Fragment</td>
<td>Total number of frames transmitted that were less than 64 octets long and had invalid CRCs.</td>
</tr>
<tr>
<td></td>
<td>Tx Abort</td>
<td>Total number of frames that had a link pointer parity error.</td>
</tr>
</tbody>
</table>
### Table 17  Output for monitor port counters (continued)

<table>
<thead>
<tr>
<th>Statistics Option</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>collisions</td>
<td>Single Coll</td>
<td>Total number of frames transmitted that experienced one collision before 64 bytes of the frame were transmitted on the network.</td>
</tr>
<tr>
<td></td>
<td>Multiple Coll</td>
<td>Total number of frames transmitted that experienced more than one collision before 64 bytes of the frame were transmitted on the network.</td>
</tr>
<tr>
<td></td>
<td>Excessive Coll</td>
<td>Total number of frames that experienced more than 16 collisions during transmit attempts. These frames are dropped and not transmitted.</td>
</tr>
<tr>
<td></td>
<td>Total Coll</td>
<td>Best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>receive-etherstats</td>
<td>Rx 64</td>
<td>Number of packets received that were 64 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Rx 127</td>
<td>Number of packets received that were from 65 through 127 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Rx 255</td>
<td>Number of packets received that were from 128 through 255 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Rx 511</td>
<td>Number of packets received that were from 256 through 511 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Rx 1023</td>
<td>Number of packets received that were from 512 through 1023 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Rx 1518</td>
<td>Number of packets received that were from 1024 through 1518 bytes long.</td>
</tr>
<tr>
<td>transmit-etherstats</td>
<td>Tx 64</td>
<td>Number of packets transmitted that were 64 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Tx 127</td>
<td>Number of packets transmitted that were from 65 through 127 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Tx 255</td>
<td>Number of packets transmitted that were from 128 through 255 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Tx 511</td>
<td>Number of packets transmitted that were from 256 through 511 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Tx 1023</td>
<td>Number of packets transmitted that were from 512 through 1023 bytes long.</td>
</tr>
<tr>
<td></td>
<td>Tx 1518</td>
<td>Number of packets transmitted that were from 1024 through 1518 bytes long.</td>
</tr>
</tbody>
</table>

**See Also**

- [display port counters](#) on page 123
**reset port**

Resets a port by toggling its link state and Power over Ethernet (PoE) state.

**Syntax** — `reset port port-list`

- `port-list` — List of physical ports. MSS resets all the specified ports.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — The reset command disables the port's link and PoE (if applicable) for at least 1 second, then reenables them. This behavior is useful for forcing a MAP access point that is connected to two WX switches to reboot over the link to the other switch.

**Examples** — The following command resets port 5:

```
WX1200# reset port 5
```

**See Also**

- `set port` on page 137

---

**set ap**

Configures a Distributed MAP for a MAP access point that is indirectly connected to the WX switch through an intermediate Layer 2 or Layer 3 network.

Before configuring a Distributed MAP, you must use the `set system countrycode` command to set the IEEE 802.11 country-specific regulations on the WX switch. See “set system countrycode” on page 109.

For a MAP that is directly connected to the WX switch, use the `set port type ap` command to configure a MAP access port.

**Syntax** — `set ap ap-number serial-id serial-ID model {
  ap2750 | ap3150 | ap3750 | ap3850 | ap3950 | ap7250 | ap8250 | ap8750} [radiotype {11a | 11b | 11g}]`
CHAPTER 4: PORT COMMANDS

- **ap-number** — Number for the Distributed MAP. The range of valid connection numbers depends on the WX switch model:
  - For a WX4400, you can specify a number from 1 to 256.
  - For a WX1200, you can specify a number from 1 to 30.

- **serial-id serial-ID** — MAP access point serial ID. The serial ID is listed on the MAP case. To show the serial ID using the CLI, use the `display version details` command.

- **radiotype 11a | 11b | 11g** — Radio type:
  - 11a — 802.11a
  - 11b — 802.11b
  - 11g — 802.11g
  This option applies only to single-radio models.

**Defaults** — The default values are the same as the defaults for the `set port type ap` command.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. New values for model option added in Version 4.1:
- AP3750
- AP2750

Version 6.0 renamed the `dap` command to `ap`.

**Examples** — The following command configures Distributed MAP 1 for MAP model AP2750 with serial-ID M9DE48B012F00:

```
WX4400# set ap 1 serial-id M9DE48B012F00 model ap2750
success: change accepted.
```

The following command removes Distributed MAP 1:

```
WX4400# clear ap 1
This will clear specified AP devices.
Would you like to continue? (y/n) [n]y
```

**See Also**
- `clear ap` on page 118
set port

Administratively disables or reenables a port.

Syntax

`set port {enable | disable} port-list`

- `enable` — Enables the specified ports.
- `disable` — Disables the specified ports.
- `port-list` — List of physical ports. MSS disables or reenables all the specified ports.

Defaults — All ports are enabled.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — A port that is administratively disabled cannot send or receive packets. This command does not affect the link state of the port.

Examples — The following command disables port 6:

```
WX1200# set port disable 6
success: set "disable" on port 6
```

The following command reenables the port:

```
WX1200# set port enable 6
success: set "enable" on port 6
```

See Also

- `reset port` on page 135
set port-group

Configures a load-sharing port group. All ports in the group function as a single logical link.

**Syntax** — `set port-group name group-name port-list mode {on | off}`

- `name group-name` — Alphanumeric string of up to 255 characters, with no spaces.
- `port-list` — List of physical ports. All the ports you specify are configured together as a single logical link.
- `mode {on | off}` — State of the group. Use `on` to enable the group or `off` to disable the group. The group is enabled by default.

**Defaults** — Once configured, a group is enabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can configure up to 8 ports in a port group, in any combination of ports. The port numbers do not need to be contiguous and you can use 10/100 Ethernet ports and gigabit Ethernet ports in the same port group.

After you add a port to a port group, you cannot configure port parameters on the individual port. Instead, change port parameters on the entire group. Specify the group name instead of an individual port name or number in port configuration commands.

To add or remove ports in a group that is already configured, change the mode to off, add or remove the ports, then change the mode to on.

**Examples** — The following command configures a port group named `server1` containing ports 1 through 5, and enables the link:

```
WX1200# set port-group name server1 1-5 mode on
success: change accepted.
```

The following commands disable the link for port group `server1`, change the list of ports in the group, and reenable the link:

```
WX1200# set port-group name server1 1-5 mode off
success: change accepted.
WX1200# set port-group name server1 1-4,7 mode on
success: change accepted.
```
set port media-type

Disables the fiber interface and enables the copper interface on an WX4400 gigabit Ethernet port.

**Syntax** — set port media-type **port-list rj45**

- **port-list**—List of physical ports. MSS sets the preference on all the specified ports.
- **rj45**—Uses the copper interface.

**Defaults** — The GBIC (fiber) interface is enabled, and the copper interface is disabled, by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — This command applies only to the WX4400.

If you set the port interface to RJ-45 on a port that already has an active fiber link, MSS immediately changes the link to the copper interface.

**Examples** — The following command disables the fiber interface and enables the copper interface on port 2:

```
WX4400# set port media-type 2 rj45
```

**See Also**

- clear port media-type on page 120
- display port media-type on page 129
**set port mirror**

Configures port mirroring. Port mirroring is a troubleshooting feature that copies (mirrors) traffic sent or received by a WX port (the source port) to another port (the observer) on the same WX. You can attach a protocol analyzer to the observer port to examine the source port's traffic. Both traffic directions (send and receive) are mirrored.

**Syntax** — set port mirror source-port observer observer-port

- **source-port** — Number of the port whose traffic you want to analyze. You can specify only one port.
- **observer-port** — Number of the port to which you want the switch to copy the source port's traffic.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — The switch can have one port mirroring pair (one source port and one observer port) at a time. The source port can be a network port, MAP access port, or wired authentication port. However, the observer port must be a network port, and cannot be a member of any VLAN or port group.

**Examples** — The following command sets port 2 to monitor port 1's traffic:

```
WX4400# set port 1 observer 2
```

**See Also**

- clear port name on page 120
- display port status on page 127
**set port name**

Assigns a name to a port. After naming a port, you can use the port name or number in other CLI commands.

**Syntax** — `set port port name name`

- `port` — Number of a physical port. You can specify only one port.
- `name name` — Alphanumeric string of up to 16 characters, with no spaces.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To simplify configuration and avoid confusion between a port’s number and its name, 3Com recommends that you do not use numbers as port names.

**Examples** — The following command sets the name of port 7 to **adminpool**:

```
WX1200# set port 7 name adminpool
success: change accepted.
```

**See Also**

- `clear port name` on page 120
- `display port status` on page 127

---

**set port negotiation**

Disables or reenables autonegotiation on gigabit Ethernet or 10/100 Ethernet ports.

**Syntax** — `set port negotiation port-list {enable | disable}`

- `port-list` — List of physical ports. MSS disables or reenables autonegotiation on all the specified ports.
- `enable` — Enables autonegotiation on the specified ports.
- `disable` — Disables autonegotiation on the specified ports.

**Defaults** — Autonegotiation is enabled on all Ethernet ports by default.
Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — WX1200 10/100 Ethernet ports support half-duplex and full-duplex operation.

3Com recommends that you do not configure the mode of an WX port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to an WX port in such a configuration can cause forwarding on the link to stop.

Examples — The following command disables autonegotiation on ports 3 and 5:

WX1200# set port negotiation 3,5 disable

The following command enables autonegotiation on port 2:

WX1200# set port negotiation 2 enable

---

**set port poe**

Enables or disables Power over Ethernet (PoE) on ports connected to MAP access points.

⚠️ **CAUTION:** When you set the port type for MAP use, you can enable PoE on the port. Use the WX switch’s PoE to power 3Com MAP access points only. If you enable PoE on ports connected to other devices, damage can result.

**Syntax** — set ap <apnum> port <portnum> model <ap_type> poe enable | disable

- **enable** — Enables PoE on the specified ports.
- **disable** — Disables PoE on the specified ports.

**Defaults** — PoE is disabled on network and wired authentication ports. The state on MAP access point ports depends on whether you enabled or disabled PoE when setting the port type. See **set port type ap** on page 145.

**Access** — Enabled.
**set port speed**

Changes the speed of a port.

**Syntax** — `set port speed port-list {10 | 100 | 1000 | auto}`

- **port-list** — List of physical ports. MSS sets the port speed on all the specified ports.
- **10** — Sets the port speed of a 10/100 Ethernet port to 10 Mbps and sets the operating mode to full-duplex.
- **100** — Sets the port speed of a 10/100 Ethernet port to 100 Mbps and sets the operating mode to full-duplex.
- **1000** — Sets the port speed of a gigabit Ethernet port to 1000 Mbps and sets the operating mode to full-duplex.
- **auto** — Enables a port to detect the speed and operating mode of the traffic on the link and set itself accordingly.

**Defaults** — All ports are set to auto.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
**Usage** — 3Com recommends that you do not configure the mode of a WX port so that one side of the link is set to autonegotiation while the other side is set to full-duplex. Although MSS allows this configuration, it can result in slow throughput on the link. The slow throughput occurs because the side that is configured for autonegotiation falls back to half-duplex. A stream of large packets sent to an WX port in such a configuration can cause forwarding on the link to stop.

**Examples** — The following command sets the port speed on ports 1 and 3 through 4 to 10 Mbps and sets the operating mode to full-duplex:

```
WX1200# set port speed 1,3-4 10
```

---

**set port trap**

Enables or disables Simple Network Management Protocol (SNMP) linkup and linkdown traps on an individual port.

**Syntax** — `set port trap port-list {enable | disable}`

- `port-list` — List of physical ports.
- `enable` — Enables the Telnet server.
- `disable` — Disables the Telnet server.

**Defaults** — SNMP linkup and linkdown traps are disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — The `set port trap` command overrides the global setting of the `set snmp trap` command.

The `set port type` command does not affect the global trap information displayed by the `display snmp configuration` command. For example, if you globally enable linkup and linkdown traps but then disable the traps on a single port, the `display snmp configuration` command still indicates that the traps are globally enabled.

**Examples** — The following command enables SNMP linkup and linkdown traps on ports 3 and 4:

```
WX1200# set port trap 3-4 enable
```
set port type ap

Configures an WX switch port for a MAP access point.

⚠️ **CAUTION:** When you set the port type for MAP use, you must specify the PoE state (enable or disable) of the port. Use the WX switch’s PoE to power 3Com MAP access points only. If you enable PoE on a port connected to another device, physical damage to the device can result.

Before configuring a port as a MAP access point port, you must use the `set system countrycode` command to set the IEEE 802.11 country-specific regulations on the WX switch. See “set system countrycode” on page 109.

Before changing the port type from `ap` to `wired-auth` or from `wired-auth` to `ap`, you must reset the port with the clear port type command.

**Syntax** — `set port type ap` *port-list* *model* {ap2750 | ap3150 | ap3750 | ap3850 | ap3950 | ap7250 | ap8250 | ap8750} *poe* {enable | disable} [radiotype {11a | 11b | 11g}]

- *port-list* — List of physical ports.
- *model* {ap2750 | ap3150 | ap3750 | ap3850 | ap3950 | ap7250 | ap8250 | ap8750} — MAP access point model:
- *poe enable* | *disable* — Power over Ethernet (PoE) state.
- *radiotype 11a* | *11b* | *11g* — Radio type:
  - *11a* — 802.11a
  - *11b* — 802.11b
  - *11g* — 802.11g

**Defaults** — All WX ports are network ports by default.

---

**See Also**

- *set ip snmp server* on page 228
- *set snmp community* on page 233
MAP access point models AP2750, MAP-241, and MAP-341 have a single radio that can be configured for 802.11a or 802.11b/g. Other MAP models have two radios. On two-radio models, one radio is always 802.11a. The other radio is 802.11b/g, but can be configured for 802.11b or 802.11g exclusively. If the country of operation specified by the set system countrycode command does not allow 802.11g, the default is 802.11b.

The radios in models MAP-620 require external antennas, and model MAP-262 requires an external antenna for the 802.11b/g radio. The following models have internal antennas but also have connectors for optional use of external antennas instead: AP2750, AP3150, AP3750, AP7250, AP8250, AP8750, MAP-372, MAP-372-CN, and MAP-372-JP. (Antenna support on a specific model is limited to the antennas certified for use with that model.) To specify the antenna model, use the set ap radio antennatype command.

**Access** — Enabled.


**Usage** — You cannot set a port type if the port is a member of a port VLAN. To remove a port from a VLAN, use the clear vlan command. To reset a port as a network port, use the clear port type command.

When you change port type, MSS applies default settings appropriate for the port type. Table 18 lists the default settings that MSS applies when you set a port's type to *ap*.

### Table 18  MAP Access Port Defaults

<table>
<thead>
<tr>
<th>Port Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN membership</td>
<td>Removed from all VLANs. You cannot assign a MAP access port to a VLAN. MSS automatically assigns MAP access ports to VLANs based on user traffic.</td>
</tr>
<tr>
<td>Spanning Tree Protocol (STP)</td>
<td>Not applicable</td>
</tr>
<tr>
<td>802.1X</td>
<td>Uses authentication parameters configured for users.</td>
</tr>
<tr>
<td>Port groups</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
This command does not apply to any gigabit Ethernet ports or to ports 7 and 8 on the WX1200 switch or port 3 on the WX2200 switch.

To manage a MAP access point on a switch model that does not have 10/100 Ethernet ports, use the `set ap` command to configure a Distributed MAP connection on the switch.

**Examples** — The following command sets ports 1 through 3 and port 5 for MAP access point model AP2750 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap2750 poe enable
```

This may affect the power applied on the configured ports. Would you like to continue? (y/n) [n] y

The following command sets ports 1 through 3 and port 5 for MAP access point model AP7250 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap7250 poe enable
```

This may affect the power applied on the configured ports. Would you like to continue? (y/n) [n] y

The following command sets ports 1 through 3 and port 5 for MAP access point model AP8250 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap8250 poe enable
```

This may affect the power applied on the configured ports. Would you like to continue? (y/n) [n] y

The following command sets ports 1 through 3 and port 5 for MAP access point model AP8750 and enables PoE on the ports:

```
WX1200# set port type ap 1-3,5 model ap8750 poe enable
```

This may affect the power applied on the configured ports. Would you like to continue? (y/n) [n] y

The following command resets port 5 by clearing it:

```
WX1200# clear port type 5
```

This may disrupt currently authenticated users. Are you sure? (y/n) [n] y

success: change accepted.

Table 18  MAP Access Port Defaults (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP snooping</td>
<td>Enabled as users are authenticated and join VLANs.</td>
</tr>
<tr>
<td>Maximum user sessions</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

This makes it easier to manage and configure MAP access points on switches without 10/100 Ethernet ports.
See Also

- clear ap on page 118
- clear port type on page 122
- set ap radio antennatype on page 431
- set ap on page 135
- set port type wired-auth on page 148
- set system countrycode on page 109

**set port type wired-auth**

Configures a WX switch port for a wired authentication user.

Before changing the port type from **ap** to **wired-auth** or from **wired-auth** to **ap**, you must reset the port with the **clear port type** command.

**Syntax** — set port type wired-auth *port-list* [tag *tag-list*] [max-sessions *num*] [auth-fall-thru {last-resort | none | web-portal}]

- *port-list* — List of physical ports.
- *tag-list* — One or more numbers between 1 and 4094 that subdivide a wired authentication port into virtual ports.
- *num* — Maximum number of simultaneous user sessions supported.
- *last-resort* — Automatically authenticates the user, without requiring a username and password.
- *none* — Denies authentication and prohibits the user from accessing the network over this port.
- *web-portal* — Serves the user a web page from the WX switch’s nonvolatile storage for secure login to the network.

**Defaults** — The default tag-list is null (no tag values). The default number of sessions is 1. The default falthru authentication type is none.

**Access** — Enabled.

**History**—Introduced in MSS Version 3.0. Option for WebAAA falthru authentication type changed from **web-auth** to **web-portal** in MSS Version 4.0.
Usage — You cannot set a port’s type if the port is a member of a port VLAN. To remove a port from a VLAN, use the `clear vlan` command. To reset a port as a network port, use the `clear port type` command.

When you change port type, MSS applies default settings appropriate for the port type. Table 19 lists the default settings that MSS applies when you set a port’s type to `ap`.

**Table 19  Wired Authentication Port Details**

<table>
<thead>
<tr>
<th>Port Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN membership</td>
<td>Removed from all VLANs. You cannot assign a MAP access port to a VLAN. MSS automatically assigns MAP access ports to VLANs based on user traffic.</td>
</tr>
<tr>
<td>Spanning Tree Protocol (STP)</td>
<td>Not applicable</td>
</tr>
<tr>
<td>802.1X</td>
<td>Uses authentication parameters configured for users.</td>
</tr>
<tr>
<td>Port groups</td>
<td>Not applicable</td>
</tr>
<tr>
<td>IGMP snooping</td>
<td>Enabled as users are authenticated and join VLANs.</td>
</tr>
<tr>
<td>Maximum user sessions</td>
<td>1 (one).</td>
</tr>
<tr>
<td>Fallthru authentication type</td>
<td>None</td>
</tr>
</tbody>
</table>

For 802.1X clients, wired authentication works only if the clients are directly attached to the wired authentication port, or are attached through a hub that does not block forwarding of packets from the client to the PAE group address (01:80:c2:00:00:03).

Wired authentication works in accordance with the 802.1X specification, which prohibits a client from sending traffic directly to an authenticator’s MAC address until the client is authenticated. Instead of sending traffic to the authenticator’s MAC address, the client sends packets to the PAE group address.

The 802.1X specification prohibits networking devices from forwarding PAE group address packets, because this would make it possible for multiple authenticators to acquire the same client.

For non-802.1X clients, who use MAC authentication, WebAAA, or last-resort authentication, wired authentication works if the clients are directly attached or indirectly attached.
Examples — The following command sets port 2 for a wired authentication user:

WX1200# set port type wired-auth 2
success: change accepted

The following command sets port 7 for a wired authentication user and specifies a maximum of three simultaneous user sessions:

WX1200# set port type wired-auth 7 max-sessions 3
success: change accepted

See Also

- clear port type on page 122
- set port type ap on page 145
Use virtual LAN (VLAN) commands to configure and manage parameters for individual port VLANs on network ports, and to display information about clients roaming within a mobility domain.

**Commands by usage**

This chapter presents VLAN commands alphabetically. Use Table 20 to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation</td>
<td>set security L2-restrict on page 171</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear security L2-restrict on page 153</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display vlan config on page 166</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>set vlan port on page 173</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display roaming station on page 161</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display roaming vlan on page 163</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display security L2-restrict on page 164</td>
<td></td>
</tr>
<tr>
<td>Roaming and Tunnels</td>
<td>set security L2-restrict on page 171</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear security L2-restrict on page 153</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display security L2-restrict counters on page 154</td>
<td></td>
</tr>
<tr>
<td>Restriction of Client</td>
<td>set security L2-restrict on page 171</td>
<td></td>
</tr>
<tr>
<td>Layer 2 Forwarding</td>
<td>display security L2-restrict on page 164</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear security L2-restrict on page 153</td>
<td></td>
</tr>
<tr>
<td>Tunnel Affinity</td>
<td>set vlan tunnel-affinity on page 174</td>
<td></td>
</tr>
<tr>
<td>FDB Entries</td>
<td>set fdb on page 169</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display fdb on page 157</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display fdb count on page 160</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear fdb on page 152</td>
<td></td>
</tr>
<tr>
<td>FDB Aging Timeout</td>
<td>set fdb agingtime on page 170</td>
<td></td>
</tr>
</tbody>
</table>
clear fdb

Deletes an entry from the forwarding database (FDB).

**Syntax** — `clear fdb {perm | static | dynamic | port port-list} [vlan vlan-id] [tag tag-value]`

- **perm** — Clears permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
- **static** — Clears static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle. You must specify a VLAN name or number with this option.
- **dynamic** — Clears dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle. You are not required to specify a VLAN name or number with this option.
- **port port-list** — Clears dynamic entries that match destination ports in the port list. You are not required to specify a VLAN name or number with this option.
- **vlan vlan-id** — VLAN name or number—required for removing permanent and static entries. For dynamic entries, specifying a VLAN removes entries that match only that VLAN. Otherwise, dynamic entries that match all VLANs are removed.
- **tag tag-value** — VLAN tag value that identifies a virtual port. If you do not specify a tag value, MSS deletes only entries that match untagged interfaces. Specifying a tag value deletes entries that match only the specified tagged interfaces

**Defaults** — None.

**Access** — Enabled.
**clear security L2-restrict**

Removes one or more MAC addresses from the list of destination MAC addresses to which clients in a VLAN are allowed to send traffic at Layer 2.

**Syntax** — `clear security L2-restrict vlan vlan-id [permit-mac mac-addr [mac-addr] | all]`

- `vlan-id` — VLAN name or number.
- `permit-mac` — List of MAC addresses. MSS no longer allows clients in the VLAN to send traffic to the MAC addresses at Layer 2.
- `all` — Removes all MAC addresses from the list.

**Defaults** — If you do not specify a list of MAC addresses or `all`, all addresses are removed.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can delete forwarding database entries based on entry type, port, or VLAN. A VLAN name or number is required for deleting permanent or static entries.

**Examples** — The following command clears all static forwarding database entries that match VLAN `blue`:

```plaintext
WX4400# clear fdb static vlan blue
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match all VLANs:

```plaintext
WX4400# clear fdb dynamic
success: change accepted.
```

The following command clears all dynamic forwarding database entries that match ports 3 and 5:

```plaintext
WX4400# clear fdb port 3,5
success: change accepted.
```

**See Also**
- `display fdb` on page 157
- `set fdb` on page 169
Access — Enabled.

History — Introduced in MSS Version 4.1.

Usage — If you clear all MAC addresses, Layer 2 forwarding is no longer restricted in the VLAN. Clients within the VLAN will be able to communicate directly.

To clear the statistics counters without removing any MAC addresses, use the `clear security L2-restrict counters` command instead.

Examples — The following command removes MAC address aa:bb:cc:dd:ee:ff from the list of addresses to which clients in VLAN abc_air are allowed to send traffic at Layer 2:

```
WX4400# clear security L2-restrict vlan abc_air permit-mac aa:bb:cc:dd:ee:ff
success: change accepted.
```

See Also

- `clear security L2-restrict counters` on page 154
- `clear security L2-restrict` on page 153
- `display security L2-restrict` on page 164

---

**clear security L2-restrict counters**

Clears statistics counters for Layer 2 forwarding restriction.

Syntax — `clear security L2-restrict counters [vlan vlan-id | all]`

- `vlan-id` — VLAN name or number.
- `all` — Clears Layer 2 forwarding restriction counters for all VLANs.

Defaults — If you do not specify a VLAN or `all`, counters for all VLANs are cleared.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Usage — To clear MAC addresses from the list of addresses to which clients are allowed to send data, use the `clear security L2-restrict` command instead.
Examples — The following command clears Layer 2 forwarding restriction statistics for VLAN abc_air:

WX4400# clear security L2-restrict counters vlan abc_air
success: change accepted.

See Also
- clear security L2-restrict on page 153
- set security L2-restrict on page 171
- display security L2-restrict on page 164

clear vlan
Removes physical or virtual ports from a VLAN or removes a VLAN entirely.

CAUTION: When you remove a VLAN, MSS completely removes the VLAN from the configuration and also removes all configuration information that uses the VLAN. If you want to remove only a specific port from the VLAN, make sure you specify the port number in the command.

Syntax — clear vlan vlan-id [port port-list [tag tag-value]]
- vlan-id — VLAN name or number.
- port port-list — List of physical ports. MSS removes the specified ports from the VLAN. If you do not specify a list of ports, MSS removes the VLAN entirely.
- tag tag-value — Tag number that identifies a virtual port. MSS removes only the specified virtual port from the specified physical ports.

Defaults — None.
Access — Enabled.
History — Introduced in MSS Version 3.0.
Usage — If you do not specify a port-list, the entire VLAN is removed from the configuration.

You cannot delete the default VLAN but you can remove ports from it. To remove ports from the default VLAN, use the port port-list option.
**Examples** — The following command removes port 1 from VLAN *green*:

WX4400# clear vlan green port 1
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.

The following command removes port 4, which uses tag value 69, from VLAN *red*:

WX1200# clear vlan red port 4 tag 69
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.

The following command completely removes VLAN *marigold*:

WX4400# clear vlan marigold
This may disrupt user connectivity.
Do you wish to continue? (y/n) [n]y
success: change accepted.

**See Also**

- *set vlan port* on page 173
- *display vlan config* on page 166

---

**clear vlan-profile**  
Removes a VLAN profile or individual entries from a VLAN profile.

**Syntax** — `clear vlan-profile profile-name [vlan vlan-name]`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — A VLAN profile lists the VLANs for which traffic is locally switched by MAPs where the VLAN profile is applied. Use this command to remove individual VLANs from a VLAN profile, or to remove an entire VLAN profile. If you remove all of the entries from a VLAN profile, the VLAN profile itself is removed.

- `profile-name`—VLAN profile name
- `vlan-name`—Name of a VLAN to remove from the VLAN profile.
If a VLAN profile is changed so that traffic that had been tunneled to an VX switch is now locally switched by MAPs, or vice-versa, the sessions of clients associated with the MAPs where the VLAN profile is applied are terminated, and the clients must re-associate with the MAPs.

**Examples** — The following command removes the entry for VLAN *red* from VLAN profile *locals*:

```plaintext
WX# clear vlan-profile locals vlan red
WX#
```

The following command removes VLAN profile *locals*:

```plaintext
WX# clear vlan-profile locals
WX#
```

**See Also**

- [display vlan-profile on page 168](#)
- [set ap local-switching vlan-profile on page 428](#)
- [set vlan profile on page 175](#)
- [display vlan-profile on page 168](#)

---

**display fdb**

Displays entries in the forwarding database.

**Syntax** — `display fdb [mac-addr-glob [vlan vlan-id ]]

- `mac-addr-glob` — A single MAC address or set of MAC addresses. Specify a MAC address, or use the wildcard character (*) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 79.)
- `vlan vlan-id` — Name or number of a VLAN for which to display entries.
- `perm` — Displays permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- `static` — Displays static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
- **dynamic** — Displays dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.

- **system** — Displays system entries. A system entry is added by MSS. For example, the authentication protocols can add entries for wired and wireless authentication users.

- **all** — Displays all entries in the database, or all the entries that match a particular port or ports or a particular VLAN.

- **port port-list** — Destination port(s) for which to display entries.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Usage** — To display the entire forwarding database, enter the `display fdb` command without options. To display only a portion of the database, use optional parameters to specify the types of entries you want to display.

**Examples** — The following command displays all entries in the forwarding database:

```
WX4400# display fdb all
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG Dest MAC/Route Des [CoS] Destination Ports [Protocol Type]
---- ---- ------------------ -----  -----------------------------------------
1  00:01:97:13:0b:1f               1                       [ALL]
1  aa:bb:cc:dd:ee:ff      *        3                       [ALL]
1  00:0b:0e:02:76:f5               1                       [ALL]
Total Matching FDB Entries Displayed = 3
```

The top line of the display identifies the characters to distinguish among the entry types.

The following command displays all entries that begin with the MAC address glob 00:

```
WX4400# display fdb 00:*
* = Static Entry. + = Permanent Entry. # = System Entry.
VLAN TAG Dest MAC/Route Des [CoS] Destination Ports [Protocol Type]
---- ---- ------------------ -----  -----------------------------------------
1  00:01:97:13:0b:1f               1                       [ALL]
1  00:0b:0e:02:76:f5               1                       [ALL]
Total Matching FDB Entries Displayed = 2
```
Table 21 describes the fields in the display fdb output.

### Table 21 Output for display fdb

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>TAG</td>
<td>VLAN tag value. If the interface is untagged, the TAG field is blank.</td>
</tr>
<tr>
<td>Dest MAC/Route Des</td>
<td>MAC address of this forwarding entry’s destination.</td>
</tr>
<tr>
<td>CoS</td>
<td>Type of entry. The entry types are explained in the first row of the command output.</td>
</tr>
<tr>
<td></td>
<td>Note: This Class of Service (CoS) value is not associated with MSS quality of service (QoS) features.</td>
</tr>
<tr>
<td>Destination Ports</td>
<td>Wireless LAN switch port associated with the entry. A WX switch sends traffic to the destination MAC address through this port.</td>
</tr>
<tr>
<td>Protocol Type</td>
<td>Layer 3 protocol address types that can be mapped to this entry.</td>
</tr>
<tr>
<td>Total Matching FDB Entries Displayed</td>
<td>Number of entries displayed by the command.</td>
</tr>
</tbody>
</table>

### See Also

- clear fdb on page 152
- set fdb on page 169

**display fdb agingtime**

Displays the aging timeout period for forwarding database entries.

**Syntax** — display fdb agingtime [vlan vlan-id]

- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, the aging timeout period for each VLAN is displayed.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays the aging timeout period for all VLANs:

```console
WX1200# display fdb agingtime
```
VLAN 2 aging time = 600 sec
VLAN 1 aging time = 300 sec

Because the forwarding database aging timeout period can be configured only on an individual VLAN basis, the command lists the aging timeout period for each VLAN separately.

**See Also**
- `set fdb agingtime` on page 170

---

**display fdb count**

Lists the number of entries in the forwarding database.

**Syntax**
```
display fdb count {perm | static | dynamic} [vlan vlan-id]
```

- `perm` — Lists the number of permanent entries. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- `static` — Lists the number of static entries. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
- `dynamic` — Lists the number of dynamic entries. A dynamic entry is automatically removed through aging or after a reboot, reset, or power cycle.
- `vlan vlan-id` — VLAN name or number. Entries are listed for only the specified VLAN.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

The following command lists the number of dynamic entries that the forwarding database contains:

```
WX1200# display fdb count dynamic
Total Matching Entries = 2
```

**See Also**
- `display fdb` on page 157
**display roaming station**

Shows a list of the stations roaming to the wireless LAN switch through a VLAN tunnel.

**Syntax** — `display roaming station`

- `[vlan vlan-id]` [peer ip-addr]
  - `vlan vlan-id` — Output is restricted to stations using this VLAN.
  - `peer ip-addr` — Output is restricted to stations tunnelling through this peer WX switch in the Mobility Domain.

**Defaults** — None.

**Access** — Enabled.


**Usage** — The output displays roaming stations within the previous 1 second.

**Examples** — To display all stations roaming to the WX switch, type the following command:

```
WX4400# display roaming station
```

<table>
<thead>
<tr>
<th>User Name</th>
<th>Station Address</th>
<th>VLAN</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>redsqa</td>
<td>10.10.10.5</td>
<td>violet</td>
<td>Up</td>
</tr>
</tbody>
</table>

Table 22 describes the fields in the display.

**Table 22** Output for display roaming station

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Name of the user. This is the name used for authentication. The name resides in a RADIUS server database or the local user database on a wireless LAN switch.</td>
</tr>
<tr>
<td>Station Address</td>
<td>IP address of the user device.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Name of the VLAN to which the RADIUS server or WX switch local user database assigned the user.</td>
</tr>
</tbody>
</table>
Table 22  Output for display roaming station (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the session:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Setup</strong> — Station is attempting to roam to this WX switch. This switch has asked the WX from which the station is roaming for the station’s session information and is waiting for a reply.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Up</strong> — MSS has established a tunnel between the WX switches and the station has successfully roamed to this WX over the tunnel.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Chck</strong> — This WX switch is in the process of accepting a reassociation request from the roaming peer WX switch for a station currently roaming to the peer switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>TChck</strong> — This WX switch is in the process of accepting a reassociation request from the roaming peer WX switch for a station currently roaming to this switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wind</strong> — This WX switch is waiting for network congestion to clear before sending the roaming indication to the roaming peer WX switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>WResp</strong> — This WX switch is waiting for network congestion to clear before sending the roaming response to the roaming peer WX switch.</td>
</tr>
</tbody>
</table>

See Also

- display roaming vlan on page 163
display roaming vlan

Shows all VLANs in the mobility domain, the WX switches servicing the VLANs, and their tunnel affinity values configured on each switch for the VLANs.

Syntax — display roaming vlan

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command shows the current roaming VLANs:

```
WX4400# display roaming vlan
VLAN             WX  Affinity
---------------- --------------- --------
vlan-cs          192.168.14.2           5
vlan-eng         192.168.14.4           5
vlan-fin         192.168.14.2           5
vlan-it          192.168.14.4           5
vlan-it          192.168.14.2           5
vlan-pm          192.168.14.2           5
vlan-sm          192.168.14.2           5
vlan-tp          192.168.14.4           5
vlan-tp          192.168.14.2           5
```

Table 23 describes the fields in the display.

Table 23  Output for display roaming vlan

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN name.</td>
</tr>
<tr>
<td>WX</td>
<td>System IP address of the wireless LAN switch on which the VLAN is configured.</td>
</tr>
<tr>
<td>Affinity</td>
<td>Preference of this WX switch for forwarding user traffic for the VLAN. A higher number indicates a greater preference.</td>
</tr>
</tbody>
</table>

See Also

- display roaming station on page 161
- display vlan config on page 166
display security L2-restrict Displays configuration information and statistics for Layer 2 forwarding restriction.

**Syntax** — display security L2-restrict [vlan vlan-id | all]

*vlan-id* — VLAN name or number.

*all* — Displays information for all VLANs.

**Defaults** — If you do not specify a VLAN name or all, information is displayed for all VLANs.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.1.

**Examples** — The following command shows Layer 2 forwarding restriction information for all VLANs:

```
VLAN Name  En  Drops  Permit MAC                  Hits
------- ----------- ---------- ------------------- ----------
 1 default  Y        0 00:0b:0e:02:53:3e         5947
             00:30:b6:3e:5c:a8            9
 2 vlan-2   Y        0 04:04:04:04:04:04:04:04  0
```

Table 24 describes the fields in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Name</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name.</td>
</tr>
<tr>
<td>En</td>
<td>Enabled state of the feature for the VLAN:</td>
</tr>
<tr>
<td></td>
<td>• Y — Enabled. Forwarding of Layer 2 traffic from clients is restricted to the MAC address(es) listed under Permit MAC.</td>
</tr>
<tr>
<td></td>
<td>• N — Disabled. Layer 2 forwarding is not restricted.</td>
</tr>
<tr>
<td>Drops</td>
<td>Number of packets dropped because the destination MAC address was not one of the addresses listed under Permit MAC.</td>
</tr>
<tr>
<td>Permit MAC</td>
<td>MAC addresses to which clients in the VLAN are allowed to send traffic at Layer 2.</td>
</tr>
</tbody>
</table>
**display tunnel**

Shows the tunnels from the wireless LAN switch where you type the command.

**Syntax** — display tunnel

**Defaults** — None.

**Access** — Enabled

**History** — Introduced in MSS Version 3.0.

**Examples** — To display all tunnels from a WX switch to other WX switches in the Mobility Domain, type the following command.

```
WX4400# display tunnel
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Local Address</th>
<th>Remote Address</th>
<th>State</th>
<th>Port</th>
<th>LVID</th>
<th>RVID</th>
</tr>
</thead>
</table>

Table 25 describes the fields in the display.

**Table 24**  Output for display security L2-restrict

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hits</td>
<td>Number of packets whose source MAC address was a client in this VLAN, and whose destination MAC address was one of those listed under Permit MAC.</td>
</tr>
</tbody>
</table>

**See Also**

- clear security L2-restrict on page 153
- clear security L2-restrict counters on page 154
- set security L2-restrict on page 171

**Table 25**  Output for display tunnel

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN name.</td>
</tr>
<tr>
<td>Local Address</td>
<td>IP address of the local end of the tunnel. This is the system IP address of the wireless access switch where you enter the command.</td>
</tr>
</tbody>
</table>
CHAPTER 5: VLAN COMMANDS

See Also
- display vlan config on page 166

display vlan config

Shows VLAN information.

**Syntax** — `display vlan config [vlan-id]`
- `vlan-id` — VLAN name or number. If you do not specify a VLAN, information for all VLANs is displayed.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays information for VLAN `burgundy`

```
WX1200# display vlan config burgundy
```

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Admin Status</th>
<th>VLAN Status</th>
<th>Tunnel Status</th>
<th>VLAN Port</th>
<th>Tag</th>
<th>Port State</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Up</td>
<td>Up</td>
<td></td>
<td>5</td>
<td>none</td>
<td>Up</td>
</tr>
<tr>
<td>4</td>
<td>none Up</td>
<td>none Up</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>none Up</td>
<td>none Up</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4094 web-aaa</td>
<td>Up</td>
<td>Up</td>
<td>0</td>
<td>2</td>
<td>4094 Up</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>t:10.10.40.4</td>
<td>none Up</td>
<td></td>
</tr>
</tbody>
</table>

Table 25  Output for display tunnel (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Address</td>
<td>IP address of the remote end of the tunnel. This is the system IP address of another WX switch in the mobility domain.</td>
</tr>
<tr>
<td>State</td>
<td>Tunnel state:</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Dormant</td>
</tr>
<tr>
<td>Port</td>
<td>Tunnel port ID.</td>
</tr>
<tr>
<td>LVID</td>
<td>Local VLAN ID.</td>
</tr>
<tr>
<td>RVID</td>
<td>Remote VLAN ID.</td>
</tr>
</tbody>
</table>
Table 26 describes the fields in this display.

**Table 26** Output for display vlan config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Administrative status of the VLAN:</td>
</tr>
<tr>
<td></td>
<td>* Down — The VLAN is disabled.</td>
</tr>
<tr>
<td></td>
<td>* Up — The VLAN is enabled.</td>
</tr>
<tr>
<td>VLAN State</td>
<td>Link status of the VLAN:</td>
</tr>
<tr>
<td></td>
<td>* Down — The VLAN is not connected.</td>
</tr>
<tr>
<td></td>
<td>* Up — The VLAN is connected.</td>
</tr>
<tr>
<td>Tunl Affin</td>
<td>Tunnel affinity value assigned to the VLAN.</td>
</tr>
<tr>
<td>Port</td>
<td>Member port of the VLAN. The port can be a physical port or a virtual port.</td>
</tr>
<tr>
<td></td>
<td>* Physical ports are 10/100 Ethernet or gigabit Ethernet ports on the WX switch, and are listed by port number.</td>
</tr>
<tr>
<td></td>
<td>* Virtual ports are tunnels to other WX switches in a mobility domain, and are listed as follows: t:ip-addr, where ip-addr is the system IP address of the WX switch at the other end of the tunnel.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field can include MAP access ports and wired authentication ports, because MSS dynamically adds these ports to a VLAN when handling user traffic for the VLAN.</td>
</tr>
<tr>
<td>Tag</td>
<td>Tag value assigned to the port.</td>
</tr>
<tr>
<td>Port State</td>
<td>Link state of the port:</td>
</tr>
<tr>
<td></td>
<td>* Down — The port is not connected.</td>
</tr>
<tr>
<td></td>
<td>* Up — The port is connected.</td>
</tr>
</tbody>
</table>

**See Also**

- `clear security L2-restrict` on page 153
- `set security L2-restrict` on page 171
- `set vlan port` on page 173
- `set vlan tunnel-affinity` on page 174
display vlan-profile

Displays the contents of the VLAN profiles configured on the WX switch. A VLAN profile lists the VLANs for which traffic is locally switched by MAPs where the VLAN profile is applied.

**Syntax** — `display vlan-profile [profile-name]`
- `profile-name` — VLAN profile name

**Defaults** — If a `profile-name` is not specified, the contents of all VLAN profiles configured on the WX switch are displayed.

**Access** — All.

**History** — Introduced in MSS Version 6.0.

**Examples** — The following command displays the contents of VLAN profile `locals`:

```
WX# display vlan-profile locals
vlan-profile: locals
Vlan Name       Tag
---------------------
blue            none
red             45
ap numbers: 67
```

Table 27 describes the fields in the `display vlan-profile` output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-profile</td>
<td>Name of the VLAN profile.</td>
</tr>
<tr>
<td>Vlan Name</td>
<td>Name of the VLAN for which local switching is performed.</td>
</tr>
<tr>
<td>Mode</td>
<td>Value of the 802.1Q tag used for the VLAN.</td>
</tr>
<tr>
<td>ap numbers</td>
<td>The index numbers of the APs where this VLAN profile is applied.</td>
</tr>
</tbody>
</table>

**See Also**
- `clear vlan-profile` on page 156
- `set ap local-switching vlan-profile` on page 428
- `set vlan profile` on page 175
set fdb

Adds a permanent or static entry to the forwarding database.

Syntax — set fdb {perm | static} mac-addr port port-list vlan vlan-id [tag tag-value]

- perm — Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- static — Adds a static entry. A static entry does not age out, but is removed from the database after a reboot, reset, or power cycle.
- mac-addr — Destination MAC address of the entry. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- port port-list — List of physical destination ports for which to add the entry. A separate entry is added for each port you specify.
- vlan vlan-id — Name or number of a VLAN of which the port is a member. The entry is added only for the specified VLAN.
- tag tag-value — VLAN tag value that identifies a virtual port. You can specify a number from 1 through 4095. If you do not specify a tag value, an entry is created for an untagged interface only. If you specify a tag value, an entry is created only for the specified tagged interface.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add a multicast or broadcast address as a permanent or static FDB entry.

Examples — The following command adds a permanent entry for MAC address 00:11:22:aa:bb:cc on ports 3 and 5 in VLAN blue:

WX1200# set fdb perm 00:11:22:aa:bb:cc port 3,5 vlan blue
success: change accepted.

The following command adds a static entry for MAC address 00:2b:3c:4d:5e:6f on port 1 in the default VLAN:

WX4400# set fdb static 00:2b:3c:4d:5e:6f port 1 vlan default
success: change accepted.
CHAPTER 5: VLAN COMMANDS

See Also

- `clear fdb` on page 152
- `display fdb` on page 157

**set fdb agingtime**

Changes the aging timeout period for dynamic entries in the forwarding database.

**Syntax** — `set fdb agingtime vlan-id age seconds`

- `vlan-id` — VLAN name or number. The timeout period change applies only to entries that match the specified VLAN.

- `age seconds` — Value for the timeout period, in seconds. You can specify a value from 0 through 1,000,000. If you change the timeout period to 0, aging is disabled.

**Defaults** — The aging timeout period is 300 seconds (5 minutes).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command changes the aging timeout period to 600 seconds for entries that match VLAN `orange`:

```
WX4400# set fdb agingtime orange age 600
success: change accepted.
```

See Also

- `display fdb agingtime` on page 159
set security L2-restrict

Restricts Layer 2 forwarding between clients in the same VLAN. When you restrict Layer 2 forwarding in a VLAN, MSS allows Layer 2 forwarding only between a client and a set of MAC addresses, generally the VLAN’s gateway routers. Clients within the VLAN are not permitted to communicate among themselves directly. To communicate with another client, the client must use one of the specified gateway routers.

**Syntax** — `set security L2-restrict vlan vlan-id [mode {enable | disable}] [permit-mac mac-addr [mac-addr]]`

- `vlan-id` — VLAN name or number.
- `mode` — Enables or disables restriction of Layer 2 forwarding.
  - `{enable | disable}`
- `permit-mac mac-addr` — MAC addresses to which clients are allowed to forward data at Layer 2. You can specify up to four addresses.

**Defaults** — Layer 2 restriction is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.1.

**Usage** — You can specify multiple addresses by listing them on the same command line or by entering multiple commands. To change a MAC address, use the `clear security L2-restrict` command to remove it, then use the `set security L2-restrict` command to add the correct address.

Restriction of client traffic does not begin until you enable the permitted MAC list. Use the `mode enable` option with this command.

**Examples** — The following command restricts Layer 2 forwarding of client data in VLAN `abc_air` to the gateway routers with MAC address `aa:bb:cc:dd:ee:ff` and `11:22:33:44:55:66`:

```
success: change accepted.
```

**See Also**
- `clear security L2-restrict` on page 153
- `clear security L2-restrict counters` on page 154
- `display security L2-restrict` on page 164
set vlan name

Creates a VLAN and assigns a number and name to it.

Syntax — *set vlan vlan-num name name*

- *vlan-num* — VLAN number. You can specify a number from 2 through 4093.
- *name* — String up to 16 alphabetic characters long.

Defaults — VLAN 1 is named `default` by default. No other VLANs have default names.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must assign a name to a VLAN (other than the default VLAN) before you can add ports to the VLAN.

3Com recommends that you do not use the name `default`. This name is already used for VLAN 1. 3Com also recommends that you do not rename the default VLAN.

You cannot use a number as the first character in a VLAN name. It is recommended that you do not use the same name with different capitalizations for VLANs. For example, do not configure two separate VLANs with the names `red` and `RED`.

VLAN names are case-sensitive for RADIUS authorization when a client roams to a wireless LAN switch. If the WX switch is not configured with the VLAN the client is on, but is configured with a VLAN that has the same spelling but different capitalization, authorization for the client fails. For example, if the client is on VLAN `red` but the WX switch to which the client roams has VLAN `RED` instead, RADIUS authorization fails.

Examples — The following command assigns the name `marigold` to VLAN 3:

```
WX4400# set vlan 3 name marigold
success: change accepted.
```

See Also

- `set vlan port` on page 173
Assigns one or more network ports to a VLAN. You also can add a virtual port to each network port by adding a tag value to the network port.

**Syntax** — `set vlan vlan-id port port-list [tag tag-value]`
- `vlan-id` — VLAN name or number.
- `port port-list` — List of physical ports.
- `tag tag-value` — Tag value that identifies a virtual port. You can specify a value from 1 through 4093.

By default, no ports are members of any VLANs. A wireless LAN switch cannot forward traffic on the network until you configure VLANs and add network ports to the VLANs.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can combine this command with the `set port name` command to assign the name and add the ports at the same time.

If you do not specify a tag value, the WX switch sends untagged frames for the VLAN. If you do specify a tag value, the WX sends tagged frames only for the VLAN.

If you do specify a tag value, 3Com recommends that you use the same value as the VLAN number. MSS does not require the VLAN number and tag value to be the same but some other switches do.

**Examples** — The following command assigns the name *beige* to VLAN 11 and adds ports 1 through 3 to the VLAN:

```
WX1200# set vlan 11 name beige port 1-3
success: change accepted.
```

The following command adds port 6 to VLAN *beige* and assigns tag value 86 to the port:

```
WX1200# set vlan beige port 6 tag 86
success: change accepted.
```

**See Also**
- `clear security L2-restrict` on page 153
- `display vlan config` on page 166
- `set security L2-restrict` on page 171
**set vlan tunnel-affinity**

Changes a wireless LAN switch’s preferability within a mobility domain for tunneling user traffic for a VLAN. When a user roams to a WX switch that is not a member of the user’s VLAN, the WX can forward the user traffic by tunneling to another WX switch that is a member of the VLAN.

**Syntax** — `set vlan vlan-id tunnel-affinity num`

- `vlan-id` — VLAN name or number.
- `num` — Preference of this switch for forwarding user traffic for the VLAN. You can specify a value from 1 through 10. A higher number indicates a greater preference.

**Defaults** — Each VLAN on a WX switch’s network ports has an affinity value of 5 by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Increasing a WX switch’s affinity value increases the WX’s preferability for forwarding user traffic for the VLAN.

If more than one WX switch has the highest affinity value, MSS randomly selects one of the WX switches for the tunnel.

**Examples** — The following command changes the VLAN affinity for VLAN `beige` to 10:

```
WX4400# set vlan beige tunnel-affinity 10
success: change accepted.
```

**See Also**

- `display roaming vlan` on page 163
- `display vlan config` on page 166
**set vlan profile**

Configures entries in a VLAN profile that can be applied to an MAP for local switching.

**Syntax** — `set vlan-profile profile-name vlan vlan-name [tag tag-value]`

- `profile-name` — VLAN profile name.
- `vlan-name` — Name of a VLAN.
- `tag-value` — Optional tag value associated with the VLAN. When this value is set, it is used as the 802.1Q tag for the VLAN.

**Defaults** — If local switching is enabled on a MAP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named `default` that is not tagged.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to a MAP, traffic for the VLANs specified in the VLAN profile is locally switched by the MAP instead of being tunneled back to an WX switch.

You enter a separate `set vlan-profile` command for each VLAN you want to add to the VLAN profile. A VLAN profile can contain up to 128 entries.

**Examples** — The following command adds an entry for VLAN `red` to VLAN profile `locals`:

```
WX# set vlan-profile locals vlan red
success: change accepted.
```

**See Also**

- `display fdb` on page 157
- `display vlan-profile` on page 168
- `clear vlan-profile` on page 156
Use Quality of Service (QoS) commands to configure packet prioritization in MSS. Packet prioritization ensures that WX switches and MAP access points give preferential treatment to high-priority traffic such as voice and video.

(To override the prioritization for specific traffic, use access controls lists [ACLs] to set the Class of Service [CoS] for the packets. See “Security ACL Commands” on page 585.)

### Commands by Usage

This chapter presents QOS commands alphabetically. Use Table 28 to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>QOS Settings</td>
<td>display qos</td>
<td>181</td>
</tr>
<tr>
<td></td>
<td>display qos dscp-table</td>
<td>182</td>
</tr>
<tr>
<td></td>
<td>set qos cos-to-dscp-map</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>set qos dscp-to-cos-map</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>clear qos</td>
<td>177</td>
</tr>
</tbody>
</table>

#### clear qos

Resets the switch's mapping of Differentiated Services Code Point (DSCP) values to internal QoS values.

The switch's internal QoS map ensures that prioritized traffic remains prioritized while transiting through the WX switch. A WX switch uses the QoS map to do the following:
Classify inbound packets by mapping their DSCP values to one of eight internal QoS values

Classify outbound packets by marking their DSCP values based on the switch’s internal QoS values

Syntax — clear qos [cos-to-dscp-map [from-qos] | dscp-to-cos-map [from-dscp]]

- **cos-to-dscp-map** — Resets the mapping between the specified internal QoS value and the DSCP values with which MSS marks outbound packets. QoS values are from 0 to 7.

- **dscp-to-cos-map** — Resets the mapping between the specified range of DSCP values and internal QoS value with which MSS classifies inbound packets.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Usage — To reset all mappings to their default values, use the clear qos command without the optional parameters.

Examples — The following command resets all QoS mappings:

WX1200# clear qos
success: change accepted.

The following command resets the mapping used to classify packets with DSCP value 44:

WX1200# clear qos dscp-to-qos-map 44
success: change accepted.
**set qos cos-to-dscp-map**

Changes the value to which MSS maps an internal QoS value when marking outbound packets.

**Syntax** — `set qos cos-to-dscp-map level dscp dscp-value`

- **level** — Internal CoS value. You can specify a number from 0 to 7.
- **dscp** **dscp-value** — DSCP value. You can specify the value as a decimal number. Valid values are 0 to 63.

**Defaults** — The defaults are listed by the `display qos` command.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.1.

**Examples** — The following command maps internal CoS value 5 to DSCP value 50:

```
WX1200# set qos cos-to-dscp-map 5 dscp 50
warning: cos 5 is marked with dscp 50 which will be classified as cos 6
```

If the change results in a change to CoS, MSS displays a warning message indicating the change. In this example, packets that receive CoS 5 upon ingress will be marked with a DSCP value equivalent to CoS 6 upon egress.

**See Also**

- `set qos dscp-to-cos-map` on page 180
- `display qos` on page 181
set qos dscp-to-cos-map

Changes the internal QoS value to which MSS maps a packet’s DSCP value when classifying inbound packets.

Syntax — set qos dscp-to-cos-map dscp-range cos level

- dscp-range — You can specify the values as decimal numbers. Valid decimal values are 0 to 63. To specify a range, use the following format: 40-56. Specify the lower number first.
- cos level — Internal QoS value. You can specify a number from 0 to 7.

Defaults — The defaults are listed by the display qos command.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command maps DSCP values 40-56 to internal CoS value 6:

WX1200# set qos dscp-to-cos-map 40-56 cos 6
warning: cos 5 is marked with dscp 63 which will be classified as cos 7
warning: cos 7 is marked with dscp 56 which will be classified as cos 6

As shown in this example, if the change results in a change to CoS, MSS displays a warning message indicating the change.

See Also

- set qos cos-to-dscp-map on page 179
- display qos on page 181
**display qos**  
Displays the switch’s QoS settings.

**Syntax — display qos [default]**

- `default` — Displays the default mappings.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.1.

**Examples** — The following command displays the default QoS settings:

```
WX1200# display qos default
```

**Ingress QoS Classification Map (dscp-to-cos)**

<table>
<thead>
<tr>
<th>Ingress DSCP</th>
<th>CoS Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-09</td>
<td>0 0 0 0 0 0 0 0 0 1</td>
</tr>
<tr>
<td>10-19</td>
<td>1 1 1 1 1 1 1 2 2 2</td>
</tr>
<tr>
<td>20-29</td>
<td>2 2 2 2 2 3 3 3 3 3</td>
</tr>
<tr>
<td>30-39</td>
<td>3 3 4 4 4 4 4 4 4 4</td>
</tr>
<tr>
<td>40-49</td>
<td>5 5 5 5 5 5 5 5 5 6</td>
</tr>
<tr>
<td>50-59</td>
<td>6 6 6 6 6 6 6 7 7 7</td>
</tr>
<tr>
<td>60-63</td>
<td>7 7 7 7 7 7 7 7 7 7</td>
</tr>
</tbody>
</table>

**Egress QoS Marking Map (cos-to-dscp)**

<table>
<thead>
<tr>
<th>CoS Level</th>
<th>0 1 2 3 4 5 6 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>00-09</td>
<td>0 8 16 24 32 40 48 56</td>
</tr>
<tr>
<td>0x00</td>
<td>0x20 0x40 0x60 0x80 0xA0</td>
</tr>
<tr>
<td>0xC0</td>
<td>0xE0</td>
</tr>
</tbody>
</table>

**See Also**

- **display qos dscp-table** on page 182
display qos dscp-table

Displays a table that maps Differentiated Services Code Point (DSCP) values to their equivalent combinations of IP precedence values and IP ToS values.

**Syntax** — `display qos dscp-table`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0 as the `display security acl dscp` command and renamed in MSS Version 4.1.

**Examples** — The following command displays the table:

```
WX1200# display qos dscp-table
  DSCP dec  TOS dec  precedence  tos
    dec  hex    dec  hex
-----------------------------------------------
  0  0x00      0  0x00             0      0
  1  0x01      4  0x04             0      2
  2  0x02      8  0x08             0      4
...
  63 0x3f   252 0xfc            7     14
```

**See Also**

- `display qos` on page 181
7

IP SERVICES COMMANDS

Use IP services commands to configure and manage IP interfaces, management services, the Domain Name Service (DNS), Network Time Protocol (NTP), aliases, and to ping a host or trace a route.

<table>
<thead>
<tr>
<th>Commands by Usage</th>
<th>This chapter presents IP services commands alphabetically. Use Table 29 to locate the commands in this chapter based on their use.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 29  IP Services Commands by Usage</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Command</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>IP Interface</td>
<td>set interface on page 218</td>
</tr>
<tr>
<td></td>
<td>set interface dhcp-client on page 219</td>
</tr>
<tr>
<td></td>
<td>set interface status on page 221</td>
</tr>
<tr>
<td></td>
<td>display interface on page 200</td>
</tr>
<tr>
<td></td>
<td>display dhcp-client on page 196</td>
</tr>
<tr>
<td></td>
<td>clear interface on page 185</td>
</tr>
<tr>
<td>System IP Address</td>
<td>set system ip-address on page 251</td>
</tr>
<tr>
<td></td>
<td>clear system ip-address on page 194</td>
</tr>
<tr>
<td>IP Route</td>
<td>set ip route on page 226</td>
</tr>
<tr>
<td></td>
<td>display ip route on page 204</td>
</tr>
<tr>
<td></td>
<td>clear ip route on page 188</td>
</tr>
<tr>
<td>SSH Management</td>
<td>set ip ssh server on page 229</td>
</tr>
<tr>
<td></td>
<td>set ip ssh on page 228</td>
</tr>
<tr>
<td>Telnet Management</td>
<td>set ip telnet on page 229</td>
</tr>
<tr>
<td></td>
<td>set ip telnet server on page 230</td>
</tr>
<tr>
<td></td>
<td>display ip telnet on page 206</td>
</tr>
<tr>
<td></td>
<td>clear ip telnet on page 189</td>
</tr>
<tr>
<td>Type</td>
<td>Command</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>HTTPS Management</td>
<td><code>set ip https server</code> on page 225</td>
</tr>
<tr>
<td></td>
<td><code>display ip https</code> on page 203</td>
</tr>
<tr>
<td>DNS</td>
<td><code>set ip dns</code> on page 223</td>
</tr>
<tr>
<td></td>
<td><code>set ip dns domain</code> on page 223</td>
</tr>
<tr>
<td></td>
<td><code>set ip dns server</code> on page 224</td>
</tr>
<tr>
<td></td>
<td><code>display ip dns</code> on page 202</td>
</tr>
<tr>
<td></td>
<td><code>clear ip dns domain</code> on page 187</td>
</tr>
<tr>
<td></td>
<td><code>clear ip dns server</code> on page 187</td>
</tr>
<tr>
<td>IP Alias</td>
<td><code>set ip alias</code> on page 222</td>
</tr>
<tr>
<td></td>
<td><code>display ip alias</code> on page 201</td>
</tr>
<tr>
<td></td>
<td><code>clear ip alias</code> on page 186</td>
</tr>
<tr>
<td>Time and Date</td>
<td><code>set timedate</code> on page 252</td>
</tr>
<tr>
<td></td>
<td><code>set timezone</code> on page 253</td>
</tr>
<tr>
<td></td>
<td><code>set summertime</code> on page 250</td>
</tr>
<tr>
<td></td>
<td><code>display timedate</code> on page 213</td>
</tr>
<tr>
<td></td>
<td><code>display timezone</code> on page 213</td>
</tr>
<tr>
<td></td>
<td><code>display summertime</code> on page 212</td>
</tr>
<tr>
<td></td>
<td><code>clear timezone</code> on page 194</td>
</tr>
<tr>
<td></td>
<td><code>clear summertime</code> on page 193</td>
</tr>
<tr>
<td>NTP</td>
<td><code>set ntp</code> on page 231</td>
</tr>
<tr>
<td></td>
<td><code>set ntp server</code> on page 232</td>
</tr>
<tr>
<td></td>
<td><code>set ntp update-interval</code> on page 233</td>
</tr>
<tr>
<td></td>
<td><code>display ntp</code> on page 207</td>
</tr>
<tr>
<td></td>
<td><code>clear ntp server</code> on page 189</td>
</tr>
<tr>
<td></td>
<td><code>clear ntp update-interval</code> on page 190</td>
</tr>
<tr>
<td>ARP</td>
<td><code>set arp</code> on page 216</td>
</tr>
<tr>
<td></td>
<td><code>set arp agingtime</code> on page 217</td>
</tr>
<tr>
<td></td>
<td><code>display dhcp-client</code> on page 196</td>
</tr>
<tr>
<td>SNMP</td>
<td><code>set snmp protocol</code> on page 245</td>
</tr>
<tr>
<td></td>
<td><code>set snmp security</code> on page 246</td>
</tr>
<tr>
<td></td>
<td><code>set snmp community</code> on page 233</td>
</tr>
<tr>
<td></td>
<td><code>set snmp usm</code> on page 247</td>
</tr>
</tbody>
</table>
clear interface

Removes an IP interface.

Syntax — `clear interface vlan-id ip`
- `vlan-id` — VLAN name or number

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If the interface you want to remove is configured as the system IP address, removing the address can interfere with system tasks using the system IP address, including the following:
- Mobility domain operations

Table 29  IP Services Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping</td>
<td>ping on page 214</td>
</tr>
<tr>
<td>Telnet Client</td>
<td>telnet on page 254</td>
</tr>
<tr>
<td>Traceroute</td>
<td>traceroute on page 255</td>
</tr>
<tr>
<td>DHCP server</td>
<td>set interface dhcp-server on page 220</td>
</tr>
<tr>
<td></td>
<td>display dhcp-server on page 198</td>
</tr>
</tbody>
</table>

| clear interface | Removes an IP interface.                    |
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

Examples — The following command removes the IP interface configured on VLAN mauve:

WX1200# clear interface mauve ip
success: cleared ip on vlan mauve

See Also
- set interface on page 218
- set interface dhcp-client on page 219
- display interface on page 200

clear ip alias

Removes an alias, which is a string that represents an IP address.

Syntax — clear ip alias name

name — Alias name

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the alias server1:

WX1200# clear ip alias server1
success: change accepted.

See Also
- display ip alias on page 201
**clear ip dns domain**

Removes the default DNS domain name.

**Syntax** — `clear ip dns domain`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command removes the default DNS domain name from a WX switch:

```
WX1200# clear ip dns domain
Default DNS domain name cleared.
```

**See Also**
- `clear ip dns server` on page 187
- `display ip dns` on page 202
- `set ip dns` on page 223
- `set ip dns domain` on page 223
- `set ip dns server` on page 224

**clear ip dns server**

Removes a DNS server from a WX switch configuration.

**Syntax** — `clear ip dns server ip-addr`

- `ip-addr` — IP address of a DNS server.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command removes DNS server 10.10.10.69 from a WX configuration:

```
WX4400# clear ip dns server 10.10.10.69
success: change accepted.
```
See Also

- clear ip dns domain on page 187
- display ip dns on page 202
- set ip dns on page 223
- set ip dns domain on page 223
- set ip dns server on page 224

```
clear ip route
```

Removes a route from the IP route table.

**Syntax** — `clear ip route {default | ip-addr mask | ip-addr/mask-length} default-router`

- `default` — Default route.

  **default** is an alias for IP address 0.0.0.0/0.

- `ip-addr mask` — IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).

- `ip-addr/mask-length` — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

- `default-router` — IP address, DNS hostname, or alias of the next-hop router.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command removes the route to destination 10.10.10.68/24 through router 10.10.10.1:

```
WX1200# clear ip route 10.10.10.68/24 10.10.10.1
success: change accepted.
```

**See Also**

- display ip route on page 204
- set ip route on page 226
clear ip telnet  Resets the Telnet server TCP port number to its default value. A WX listens for Telnet management traffic on the Telnet server port.

**Syntax** — clear ip telnet

**Defaults** — The default Telnet port number is 23.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command resets the TCP port number for Telnet management traffic to its default:

```
WX4400# clear ip telnet
success: change accepted.
```

**See Also**

- display ip https on page 203
- display ip telnet on page 206
- set ip https server on page 225
- set ip telnet on page 229
- set ip telnet server on page 230

---

clear ntp server  Removes an NTP server from a WX configuration.

**Syntax** — clear ntp server {ip-addr | all}

- `ip-addr` — IP address of the server to remove, in dotted decimal notation.
- `all` — Removes all NTP servers from the configuration.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
Examples — The following command removes NTP server 192.168.40.240 from a WX switch configuration:

WX4400# clear ntp server 192.168.40.240
success: change accepted.

See Also
- **clear ntp update-interval** on page 190
- **display ntp** on page 207
- **set ntp** on page 231
- **set ntp server** on page 232
- **set ntp update-interval** on page 233

---

clear ntp update-interval

Resets the NTP update interval to the default value.

**Syntax** — *clear ntp update-interval*

**Defaults** — The default NTP update interval is 64 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

Examples — To reset the NTP interval to the default value, type the following command:

WX4400# clear ntp update-interval
success: change accepted.

See Also
- **clear ntp server** on page 189
- **display ntp** on page 207
- **set ntp** on page 231
- **set ntp server** on page 232
- **set ntp update-interval** on page 233
**clear snmp community**

Clears an SNMP community string.

**Syntax** — `clear snmp community name comm-string`

- `comm-string` — Name of the SNMP community you want to clear.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command clears community string `setswitch2`:

```
WX1200# clear snmp community name setswitch2
success: change accepted.
```

**See Also**

- `set snmp community` on page 233
- `display snmp community` on page 209

---

**clear snmp notify profile**

Clears an SNMP notification profile.

**Syntax** — `clear snmp notify profile profile-name`

- `profile-name` — Name of the notification profile you are clearing.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command clears notification profile `snmpprof_rfdetect`:

```
WX1200# clear snmp notify profile snmpprof_rfdetect
success: change accepted.
```
See Also

- set snmp notify profile on page 235
- display snmp notify profile on page 210

clear snmp notify target

Clears an SNMP notification target.

**Syntax** — `clear snmp notify target target-num`

- `target-num` — ID of the target.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command clears notification target 3:

```
WX1200# clear snmp notify target 3
success: change accepted.
```

See Also

- set snmp notify target on page 240
- display snmp notify target on page 210

clear snmp usm

Clears an SNMPv3 user.

**Syntax** — `clear snmp usm usm-username`

- `usm-username` — Name of the SNMPv3 user you want to clear.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.
clear summertime

Examples — The following command clears SNMPv3 user snmpmgr1:

WX1200# clear snmp usm snmpmgr1
success: change accepted.

See Also

- set snmp usm on page 247
- display snmp usm on page 212

clear summertime

Clears the summertime setting from a WX.

Syntax — clear summertime

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To clear the summertime setting from a WX, type the following command:

WX1200# clear summertime
success: change accepted.

See Also

- clear timezone on page 194
- display summertime on page 212
- display timedate on page 213
- display timezone on page 213
- set summertime on page 250
- set timedate on page 252
- set timezone on page 253
clear system ip-address

Clears the system IP address.

**CAUTION:** Clearing the system IP address disrupts the system tasks that use the address.

**Syntax** — `clear system ip-address`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Clearing the system IP address can interfere with system tasks that use the system IP address, including the following:

- Mobility Domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

**Examples** — To clear the system IP address, type the following command:

```
WX1200# clear system ip-address
success: change accepted.
```

**See Also**

- `display system` on page 95
- `set system ip-address` on page 251

---

clear timezone

Clears the time offset for the WX real-time clock from Coordinated Universal Time (UTC). UTC is also known as Greenwich Mean Time (GMT).

**Syntax** — `clear timezone`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
Examples — To return the WX real-time clock to UTC, type the following command:

WX4400# clear timezone
success: change accepted.

See Also
- clear summertime on page 193
- set summertime on page 250
- set timedate on page 252
- set timezone on page 253
- display summertime on page 212
- display timedate on page 213
- display timezone on page 213

display arp

Shows the ARP table.

Syntax — display arp [ip-addr]
- ip-addr — IP address.

Defaults — If you do not specify an IP address, the entire ARP table is displayed.

Usage — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays ARP entries:

WX4400# display arp
ARP aging time: 1200 seconds

<table>
<thead>
<tr>
<th>Host</th>
<th>HW Address</th>
<th>VLAN</th>
<th>Type</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.4.51</td>
<td>00:0b:0e:02:76:f5</td>
<td>1</td>
<td>DYNAMIC</td>
<td>RESOLVED</td>
</tr>
<tr>
<td>10.5.4.53</td>
<td>00:0b:0e:02:76:f7</td>
<td>1</td>
<td>LOCAL</td>
<td>RESOLVED</td>
</tr>
</tbody>
</table>
Table 30 describes the fields in this display.

**Table 30** Output for display arp

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP aging time</td>
<td>Number of seconds a dynamic entry can remain unused before MSS removes the entry from the ARP table.</td>
</tr>
<tr>
<td>Host</td>
<td>IP address, hostname, or alias.</td>
</tr>
<tr>
<td>HW Address</td>
<td>MAC address mapped to the IP address, hostname, or alias.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN the entry is for.</td>
</tr>
<tr>
<td>Type</td>
<td>Entry type:</td>
</tr>
<tr>
<td></td>
<td>- <strong>DYNAMIC</strong> — Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout.</td>
</tr>
<tr>
<td></td>
<td>- <strong>LOCAL</strong> — Entry for the WX switch’s MAC address. Each VLAN has one local entry for the WX switch’s MAC address.</td>
</tr>
<tr>
<td></td>
<td>- <strong>PERMANENT</strong> — Entry does not age out and remains in the configuration even following a reboot.</td>
</tr>
<tr>
<td></td>
<td>- <strong>STATIC</strong> — Entry does not age out but is removed after a reboot.</td>
</tr>
<tr>
<td>State</td>
<td>Entry state:</td>
</tr>
<tr>
<td></td>
<td>- <strong>RESOLVING</strong> — MSS sent an ARP request for the entry and is waiting for the reply.</td>
</tr>
<tr>
<td></td>
<td>- <strong>RESOLVED</strong> — Entry is resolved.</td>
</tr>
</tbody>
</table>

**See Also**

- **set arp** on page 216
- **set arp agingtime** on page 217

**display dhcp-client** Displays DHCP client information for all VLANs.

**Syntax** — `display dhcp-client`

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 4.0.
Examples — The following command displays DHCP client information:

```
WX1200# display dhcp-client
Interface:    corpvlan(4)
Configuration Status:  Enabled
DHCP State:    IF_UP
Lease Allocation:  65535 seconds
Lease Remaining:  65532 seconds
IP Address:     10.3.1.110
Subnet Mask:    255.255.255.0
Default Gateway: 10.3.1.1
DHCP Server:    10.3.1.4
DNS Servers:    10.3.1.29
DNS Domain Name: mycorp.com
```

Table 31 describes the fields in this display.

**Table 31  Output for display dhcp-client**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>VLAN name and number.</td>
</tr>
<tr>
<td>Configuration Status</td>
<td>Status of the DHCP client on this VLAN:</td>
</tr>
<tr>
<td></td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP State</td>
<td>State of the IP interface:</td>
</tr>
<tr>
<td></td>
<td>IF_UP</td>
</tr>
<tr>
<td></td>
<td>IF_DOWN</td>
</tr>
<tr>
<td>Lease Allocation</td>
<td>Duration of the address lease.</td>
</tr>
<tr>
<td>Lease Remaining</td>
<td>Number of seconds remaining before the address lease expires.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address received from the DHCP server</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Network mask of the IP address received from the DHCP server.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Default gateway IP address received from the DHCP server. If the address is 0.0.0.0, the server did not provide an address.</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>IP address of the DHCP server.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>DNS server IP address(es) received from the DHCP server.</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Default DNS domain name received from the DHCP server.</td>
</tr>
</tbody>
</table>

See Also

- `set interface dhcp-client` on page 219
display dhcp-server

Displays MSS DHCP server information.

**Syntax** — `display dhcp-server [interface vlan-id] [verbose]`

- `interface vlan-id` — Displays the IP addresses leased by the specified VLAN.
- `verbose` — Displays configuration and status information for the MSS DHCP server.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command displays the addresses leased by the MSS DHCP server:

```
WX1200# display dhcp-server
```

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Address</th>
<th>MAC Address</th>
<th>Lease Remaining</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.10.20.2</td>
<td>00:01:02:03:04:05</td>
<td>12345</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>10.10.20.3</td>
<td>00:01:03:04:06:07</td>
<td>2103</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>192.168.1.5</td>
<td>00:01:03:04:06:08</td>
<td>102</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>192.168.1.7</td>
<td>00:01:03:04:06:09</td>
<td>16789</td>
<td></td>
</tr>
</tbody>
</table>

The following command displays configuration and status information for each VLAN on which the DHCP server is configured:

```
WX1200# display dhcp-server verbose
```

**Interface:** 0 (Direct AP)
**Status:** UP
**Address Range:** 10.0.0.1-10.0.0.253

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Address Range</th>
<th>DHCP Clients:</th>
</tr>
</thead>
<tbody>
<tr>
<td>default(1)</td>
<td>UP</td>
<td>10.10.20.2-10.10.20.254</td>
<td></td>
</tr>
<tr>
<td>Hardware Address:</td>
<td>00:01:02:03:04:05</td>
<td>BOUND</td>
<td></td>
</tr>
<tr>
<td>Lease Allocation:</td>
<td>43200 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lease Remaining:</td>
<td>12345 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address:</td>
<td>10.10.20.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet Mask:</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Default Gateway: 10.10.20.1
DNS Servers: 10.10.20.4 10.10.20.5
DNS Domain Name: mycorp.com

Table 32 and Table 33 describe the fields in these displays.

**Table 32  Output for display dhcp-server**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN number</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name</td>
</tr>
<tr>
<td>Address</td>
<td>IP address leased by the server.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the device that holds the least for the address.</td>
</tr>
<tr>
<td>Lease Remaining</td>
<td>Number of seconds remaining before the address lease expires.</td>
</tr>
</tbody>
</table>

**Table 33  Output for display dhcp-server verbose**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>VLAN name and number.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the interface:</td>
</tr>
<tr>
<td></td>
<td>• UP</td>
</tr>
<tr>
<td></td>
<td>• DOWN</td>
</tr>
<tr>
<td>Address Range</td>
<td>Range from which the server can lease addresses.</td>
</tr>
<tr>
<td>Hardware Address</td>
<td>MAC address of the DHCP client.</td>
</tr>
<tr>
<td>Lease Remaining</td>
<td>Number of seconds remaining before the address lease expires.</td>
</tr>
<tr>
<td>State</td>
<td>State of the address lease:</td>
</tr>
<tr>
<td></td>
<td>• SUSPEND—MSS is checking for the presence of another DHCP server on the subnet. This is the initial state of the MSS DHCP server. The MSS DHCP server remains in this state if another DHCP server is detected.</td>
</tr>
<tr>
<td></td>
<td>• CHECKING—MSS is using ARP to verify whether the address is available.</td>
</tr>
<tr>
<td></td>
<td>• OFFERING—MSS offered the address to the client and is waiting for the client to send a DHCPREQUEST for the address.</td>
</tr>
<tr>
<td></td>
<td>• BOUND—The client accepted the address.</td>
</tr>
<tr>
<td></td>
<td>• HOLDING—The address is already in use and is therefore unavailable.</td>
</tr>
<tr>
<td>Lease Allocation</td>
<td>Duration of the address lease, in seconds.</td>
</tr>
<tr>
<td>Lease Remaining</td>
<td>Number of seconds remaining before the address lease expires.</td>
</tr>
</tbody>
</table>
CHAPTER 7: IP SERVICES COMMANDS

See Also
- **set interface dhcp-server** on page 220

**display interface**
Displays the IP interfaces configured on the WX.

**Syntax** — **display interface** [vlan-id]

- vlan-id — VLAN name or number.

**Defaults** — If you do not specify a VLAN ID, interfaces for all VLANs are displayed.

**Usage** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays all the IP interfaces configured on a WX switch:

```
WX4400# display interface
VLAN Name      Address      Mask          Enabled State RIB
-------------  -----------  --------------  ---------- ----
  1 default    10.10.10.10  255.255.255.0  YBS       Up    ipv4
  2 mauve      10.10.20.10  255.255.255.0  NO        Down  ipv4
4094 web-aaa  10.10.10.1   255.255.255.0  YBS       Up    ipv4
```

Table 34 describes the fields in this display.
**display ip alias**

Displays the IP aliases configured on the WX.

**Syntax** — `display ip alias [name]`

* *name* — Alias string.

**Defaults** — If you do not specify an alias name, all aliases are displayed.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays all the aliases configured on a WX switch:

```
WX4400# display ip alias
Name                  IP Address
---------------------- ----------------
HR1                   192.168.1.2
payroll               192.168.1.3
radius1               192.168.7.2
```
Table 35 describes the fields in this display.

**Table 35** Output for display ip alias

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Alias string.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address associated with the alias.</td>
</tr>
</tbody>
</table>

**See Also**

- clear ip alias on page 186
- set ip alias on page 222

**display ip dns** Displays the DNS servers used by the WX.

**Syntax** — display ip dns

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays the DNS information:

```
WX4400# display ip dns
Domain Name: example.com
DNS Status: enabled
IP Address     Type
-------------------------------
10.1.1.1        PRIMARY
10.1.1.2        SECONDARY
10.1.2.1        SECONDARY
```

Table 36 describes the fields in this display.

**Table 36** Output for display ip dns

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Default domain name configured on the WX switch</td>
</tr>
</tbody>
</table>
**display ip https**

Shows information about the HTTPS management port.

**Syntax** — `display ip https`

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command shows the status and port number for the HTTPS management interface to the WX switch:

```plaintext
WX4400# display ip https
HTTPS is enabled
HTTPS is set to use port 443
Last 10 Connections:
IP Address Last Connected Time Ago (s)
----------------- ------------------ ------------
10.10.10.56 2003/05/09 15:51:26 pst 349
```

Table 37 describes the fields in this display.

---

**Table 36** Output for `display ip dns` (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Status</td>
<td>Status of the WX switch’s DNS client:</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the DNS server</td>
</tr>
<tr>
<td>Type</td>
<td>Server type:</td>
</tr>
<tr>
<td></td>
<td>• PRIMARY</td>
</tr>
<tr>
<td></td>
<td>• SECONDARY</td>
</tr>
</tbody>
</table>

---

See Also

- `clear ip dns domain` on page 187
- `clear ip dns server` on page 187
- `set ip dns` on page 223
- `set ip dns domain` on page 223
- `set ip dns server` on page 224
Table 37  Output for display ip https

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| HTTPS is enabled/disabled | State of the HTTPS server:  
- Enabled  
- Disabled |
| HTTPS is set to use port | TCP port number on which the WX switch listens for HTTPS connections. |
| Last 10 connections | List of the last 10 devices to establish connections to the WX HTTPS server. |
| IP Address        | IP address of the device that established the HTTPS connection.  
**Note:** If a browser connects to a WX from behind a proxy, then only the proxy IP address is shown. If multiple browsers connect using the same proxy, the proxy address appears only once in the output. |
| Last Connected    | Time when the WX switch established the HTTPS connection to the WX switch. |
| Time Ago (s)      | Number of seconds since the device established the HTTPS connection to the WX switch. |

**See Also**
- `clear ip telnet` on page 189
- `display ip telnet` on page 206
- `set ip https server` on page 225
- `set ip telnet` on page 229
- `set ip telnet server` on page 230

**display ip route**
Displays the IP route table on the WX.

**Syntax** — `display ip route [destination]`
- `destination` — Route destination IP address, in dotted decimal notation.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.
**Usage** — When you add an IP interface to a VLAN that is up, MSS adds direct and local routes for the interface to the route table. If the VLAN is down, MSS does not add the routes. If you add an interface to a VLAN but the routes for that interface do not appear in the route table, use the `display vlan config` command to check the VLAN state.

If you add a static route and the route’s state is shown as Down, use the `display interface` command to verify that the route has an IP interface in the gateway router’s subnet. MSS cannot resolve a static route unless one of the WX switch’s VLANs has an interface in the gateway router’s subnet. If the WX switch has such an interface but the static route is still down, use the `display vlan config` command to check the state of the VLAN’s ports.

**Examples** — The following command shows all routes in a WX IP route table:

```
WX4400# display ip route
```

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Proto</th>
<th>Metric</th>
<th>NH-Type</th>
<th>Gateway</th>
<th>VLAN:Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>Static</td>
<td>1</td>
<td>Router</td>
<td>10.0.1.17</td>
<td>Down</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>Static</td>
<td>2</td>
<td>Router</td>
<td>10.0.2.17</td>
<td>VLAN:2:ip</td>
</tr>
<tr>
<td>10.0.2.1/24</td>
<td>IP</td>
<td>0</td>
<td>Direct</td>
<td></td>
<td>VLAN:2:ip</td>
</tr>
<tr>
<td>10.0.2.1/32</td>
<td>IP</td>
<td>0</td>
<td>Direct</td>
<td></td>
<td>VLAN:2:ip:10.0.1.1/24</td>
</tr>
<tr>
<td>10.0.2.255/32</td>
<td>IP</td>
<td>0</td>
<td>Direct</td>
<td></td>
<td>VLAN:2:ip:10.0.1.1/24</td>
</tr>
<tr>
<td>224.0.0.0/4</td>
<td>IP</td>
<td>0</td>
<td>Local</td>
<td></td>
<td>MULTICAST</td>
</tr>
</tbody>
</table>

Table 38 describes the fields in this display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination/Mask</td>
<td>IP address and subnet mask of the route destination. The 244.0.0.0 route is automatically added by MSS and supports the IGMP snooping feature.</td>
</tr>
<tr>
<td>Proto</td>
<td>Protocol that added the route to the IP route table. The protocol can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>■ IP — MSS added the route.</td>
</tr>
<tr>
<td></td>
<td>■ Static — An administrator added the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>Cost for using the route.</td>
</tr>
</tbody>
</table>
CHAPTER 7: IP SERVICES COMMANDS

See Also

- clear ip route on page 188
- display interface on page 200
- display vlan config on page 166
- set interface on page 218
- set ip route on page 226

**display ip telnet**

Shows information about the Telnet management port.

**Syntax** — display ip telnet

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.
**Examples** — The following command shows the status and port number for the Telnet management interface to the WX switch:

```
WX4400> display ip telnet
```

<table>
<thead>
<tr>
<th>Server Status</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>23</td>
</tr>
</tbody>
</table>

Table 39 describes the fields in this display.

**Table 39** Output for display ip telnet

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Status</td>
<td>State of the HTTPS server:</td>
</tr>
<tr>
<td></td>
<td>• Enabled</td>
</tr>
<tr>
<td></td>
<td>• Disabled</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port number on which the WX switch listens for Telnet management traffic.</td>
</tr>
</tbody>
</table>

**See Also**

- `clear ip telnet` on page 189
- `display ip https` on page 203
- `set ip https server` on page 225
- `set ip telnet` on page 229
- `set ip telnet server` on page 230

**display ntp**

Shows NTP client information.

**Syntax** — `display ntp`

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.
Examples — To display NTP information for a WX switch, type the following command:

WX4400> display ntp
NTP client: enabled
Current update-interval: 20 (secs)
Current time: Fri Feb 06 2004, 12:02:57
Timezone is set to 'PST', offset from UTC is -8:0 hours.
Summertime is enabled.
Last NTP update: Fri Feb 06 2004, 12:02:46
NTP Server             Peer state             Local State
---------------------------------------------------
192.168.1.5             SYSPEER                SYNCED

Table 40 describes the fields in this display.

**Table 40** Output for display ntp

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP client</td>
<td>State of the NTP client. The state can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>▪ Enabled</td>
</tr>
<tr>
<td></td>
<td>▪ Disabled</td>
</tr>
<tr>
<td>Current update-interval</td>
<td>Number of seconds between queries sent by the WX to the NTP servers for updates.</td>
</tr>
<tr>
<td>Current time</td>
<td>System time that was current on the WX when you pressed Enter after typing the display ntp command.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Time zone configured on the WX switch. MSS offsets the time reported by the NTP server based on the time zone. This field is displayed only if you change the time zone.</td>
</tr>
<tr>
<td>Summertime</td>
<td>Summertime period configured on the WX switch. MSS offsets the system time +1 hour and returns it to standard time for daylight savings time or a similar summertime period that you set. This field is displayed only if you enable summertime.</td>
</tr>
<tr>
<td>Last NTP update</td>
<td>Time when the WX received the most recent update from an NTP server.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>IP address of the NTP server.</td>
</tr>
</tbody>
</table>
**display snmp community**

Displays the configured SNMP community strings.

**Syntax** — `display snmp community`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

---

**Table 40**  Output for display ntp (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer state</td>
<td>State of the NTP session from the point of view of the NTP server:</td>
</tr>
<tr>
<td></td>
<td>- CORRECT</td>
</tr>
<tr>
<td></td>
<td>- REJECT</td>
</tr>
<tr>
<td></td>
<td>- SELCAND</td>
</tr>
<tr>
<td></td>
<td>- SYNCCAND</td>
</tr>
<tr>
<td></td>
<td>- SYSPEER</td>
</tr>
<tr>
<td>Local state</td>
<td>State of the NTP session from the point of view of the WX NTP client:</td>
</tr>
<tr>
<td></td>
<td>- INITED</td>
</tr>
<tr>
<td></td>
<td>- START</td>
</tr>
<tr>
<td></td>
<td>- SYNCED</td>
</tr>
</tbody>
</table>

**See Also**

- `clear ntp server` on page 189
- `clear summertime` on page 193
- `clear timezone` on page 194
- `display timezone` on page 213
- `set ntp` on page 231
- `set ntp server` on page 232
- `set summertime` on page 250
- `set timezone` on page 253
See Also

- clear snmp community on page 191
- set snmp community on page 233

**display snmp counters**
Displays SNMP statistics counters.

Syntax — display snmp counters

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

**display snmp notify profile**
Displays SNMP notification profiles.

Syntax — display snmp notify profile

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

See Also

- clear snmp notify profile on page 191
- set snmp notify profile on page 235

**display snmp notify target**
Displays SNMP notification targets.

Syntax — display snmp notify target

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.
**display snmp status**

Displays SNMP version and status information.

**Syntax** — `display snmp status`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**See Also**

- `set snmp community` on page 233
- `set snmp notify target` on page 240
- `set snmp notify profile` on page 235
- `set snmp protocol` on page 245
- `set snmp security` on page 246
- `set snmp usm` on page 247
- `display snmp community` on page 209
- `display snmp counters` on page 210
- `display snmp notify profile` on page 210
- `display snmp notify target` on page 210
- `display snmp usm` on page 212
display snmp usm  Displays information about SNMPv3 users.

Defaults  — None.

Access  — Enabled.

History  — Introduced in MSS Version 4.0.

See Also
- clear snmp usm on page 192
- display snmp usm on page 212

display summertime  Displays a WX offset time from its real-time clock time.

Syntax  — display summertime

Defaults  — There is no summertime offset by default.

Access  — All.

History  — Introduced in MSS Version 3.0.

Examples  — To display the summertime setting on a WX, type the following command:

WX1200# display summertime
Summertime is enabled, and set to 'PDT'.
Start : Sun Apr 04 2004, 02:00:00
End   : Sun Oct 31 2004, 02:00:00
Offset : 60 minutes
Recurring : yes, starting at 2:00 am of first Sunday of April
and ending at 2:00 am on last Sunday of October.

See Also
- clear summertime on page 193
- clear timezone on page 194
- display timedate on page 213
- display timezone on page 213
- set summertime on page 250
display timedate

Shows the date and time of day currently set on a WX real-time clock.

Syntax — display timedate

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — To display the time and date set on a WX real-time clock, type the following command:

WX1200# display timedate
Sun Feb 29 2004, 23:59:02 PST

See Also
- clear summertime on page 193
- clear timezone on page 194
- display summertime on page 212
- display timezone on page 213
- set summertime on page 250
- set timedate on page 252
- set timezone on page 253

display timezone

Displays the time offset for the real-time clock from UTC on a WX.

Syntax — display timezone

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.
Examples — To display the offset from UTC, type the following command:

WX4400# display timezone
Timezone set to 'pst', offset from UTC is -8 hours

See Also

- clear summertime on page 193
- clear timezone on page 194
- display summertime on page 212
- display timedate on page 213
- set summertime on page 250
- set timedate on page 252
- set timezone on page 253

ping

Tests IP connectivity between a WX and another device. MSS sends an Internet Control Message Protocol (ICMP) echo packet to the specified device and listens for a reply packet.

Syntax — ping host [count num-packets ] [dnf] [flood] [interval time] [size size] [source-ip ip-addr | vlan-name]

- host — IP address, MAC address, hostname, alias, or user to ping.
- count num-packets — Number of ping packets to send. You can specify from 0 through 2,147,483,647. If you enter 0, MSS pings continuously until you interrupt the command.
- dnf — Enables the Do Not Fragment bit in the ping packet to prevent fragmenting the packet.
- flood — Sends new ping packets as quickly as replies are received, or 100 times per second, whichever is greater.

Use the flood option sparingly. This option creates a lot of traffic and can affect other traffic on the network.

- interval time — Time interval between ping packets, in milliseconds. You can specify from 100 through 10,000.
- size size — Packet size, in bytes. You can specify from 56 through 65,507.
Because the WX switch adds header information, the ICMP packet size is 8 bytes larger than the size you specify.

- **source-ip ip-addr** — IP address, in dotted decimal notation, to use as the source IP address in the ping packets.
- **source-ip vlan-name** — VLAN name to use as the ping source. MSS uses the IP address configured on the VLAN as the source IP address in the ping packets.

**Defaults**

- **count** — 5.
- **dnf** — Disabled.
- **interval** — 100 (one tenth of a second)
- **size** — 56.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To stop a ping command that is in progress, press Ctrl+C.

**Examples** — The following command pings a WX switch that has IP address 10.1.1.1:

WX1200# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) from 10.9.4.34 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.769 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=255 time=0.628 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=255 time=0.676 ms
64 bytes from 10.1.1.1: icmp_seq=4 ttl=255 time=0.619 ms
64 bytes from 10.1.1.1: icmp_seq=5 ttl=255 time=0.608 ms
--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0 errors, 0% packet loss

**See Also**

- **traceroute** on page 255
set arp

Adds an ARP entry to the ARP table.

**Syntax**

```
set arp {permanent | static | dynamic } ip-addr mac-addr
```

- **permanent** — Adds a permanent entry. A permanent entry does not age out and remains in the database even after a reboot, reset, or power cycle.
- **static** — Adds a static entry. A static entry does not age out, but the entry does not remain in the database after a reboot, reset, or power cycle.
- **dynamic** — Adds a dynamic entry. A dynamic entry is automatically removed if the entry ages out, or after a reboot, reset, or power cycle.
- **ip-addr** — IP address of the entry, in dotted decimal notation.
- **mac-addr** — MAC address to map to the IP address. Use colons to separate the octets (for example, 00:11:22:aa:bb:cc).

**Defaults** — The default aging timeout is 1200 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command adds a static ARP entry that maps IP address 10.10.10.1 to MAC address 00:bb:cc:dd:ee:ff:

```
WX1200# set arp static 10.10.10.1 00:bb:cc:dd:ee:ff
success: added arp 10.10.10.1 at 00:bb:cc:dd:ee:ff on VLAN 1
```

**See Also**

- [set arp agingtime](#) on page 217
- [telnet](#) on page 254
**set arp agingtime**

Changes the aging timeout for dynamic ARP entries.

**Syntax** — `set arp agingtime seconds`

- `seconds` — Number of seconds an entry can remain unused before MSS removes the entry. You can specify from 0 through 1,000,000. To disable aging, specify 0.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Aging applies only to dynamic entries.

To reset the ARP aging timeout to its default value, use the `set arp agingtime 1200` command.

**Examples** — The following command changes the ARP aging timeout to 1800 seconds:

```
WX1200# set arp agingtime 1800
success: set arp aging time to 1800 seconds
```

The following command disables ARP aging:

```
WX1200# set arp agingtime 0
success: set arp aging time to 0 seconds
```

**See Also**

- `set arp` on page 216
- `telnet` on page 254
set interface

Configures an IP interface on a VLAN.

**Syntax** — `set interface vlan-id ip {ip-addr mask | ip-addr/mask-length}`

- `vlan-id` — VLAN name or number.
- `ip-addr mask` — IP address and subnet mask in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).
- `ip-addr/mask-length` — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can assign one IP interface to each VLAN.

If an interface is already configured on the specified VLAN, this command replaces the interface. If you replace an interface in use as the system IP address, replacing the interface can interfere with system tasks that use the system IP address, including the following:

- Mobility domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

**Examples** — The following command configures IP interface 10.10.10.10/24 on VLAN default:

```
WX1200# set interface default ip 10.10.10.10/24
success: set ip address 10.10.10.10 netmask 255.255.255.0 on vlan default
```

The following command configures IP interface 10.10.20.10 255.255.255.0 on VLAN mauve:

```
WX1200# set interface mauve ip 10.10.20.10 255.255.255.0
success: set ip address 10.10.20.10 netmask 255.255.255.0 on vlan mauve
```
**set interface dhcp-client**

Configures the DHCP client on a VLAN and allows the VLAN to obtain its IP interface from a DHCP server.

**Syntax** — `set interface vlan-id ip dhcp-client {enable | disable}`

- `vlan-id` — VLAN name or number.
- `enable` — Enables the DHCP client on the VLAN.
- `disable` — Disables the DHCP client on the VLAN.

**Defaults** — The DHCP client is enabled by default on an unconfigured WXR100 when the factory reset switch is pressed and held during power on.

The DHCP client is disabled by default on all other WX models, and is disabled on a WXR100 if it is already configured or the factory reset switch is not pressed and held during power on.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — You can enable the DHCP client on one VLAN only. You can configure the DHCP client on more than one VLAN, but the client can be active on only one VLAN.

MSS also has a configurable DHCP server. (See `set interface dhcp-server` on page 220.) You can configure a DHCP client and DHCP server on the same VLAN, but only the client or the server can be enabled. The DHCP client and DHCP server cannot both be enabled on the same VLAN at the same time.

**Examples** — The following command enables the DHCP client on VLAN corpvlan:

```
WX1200# set interface corpvlan ip dhcp-client enable
success: change accepted.
```
set interface dhcp-server

Configures the MSS DHCP server.

Use of the MSS DHCP server to allocate client addresses is intended for temporary, demonstration deployments and not for production networks. It is recommended that you do not use the MSS DHCP server to allocate client addresses in a production network.

Syntax — set interface vlan-id ip dhcp-server [enable | disable] [start ip-addr1 stop ip-addr2] [dns-domain domain-name] [primary-dns ip-addr [secondary-dns ip-addr]] [default-router ip-addr]

- `vlan-id` — VLAN name or number.
- `enable` — Enables the DHCP server.
- `disable` — Disables the DHCP server.
- `start ip-addr1` — Specifies the beginning address of the address range (also called the address pool).
- `stop ip-addr2` — Specifies the ending address of the address range.
- `dns-domain domain-name` — Name of the DHCP client’s default DNS domain.
- `default-router ip-addr` — IP address of the DHCP client’s default router.

Defaults — The DHCP server is enabled by default on a new (unconfigured) WX2500, in order to provide an IP address to the host connected to the WX for access to the Web Quick Start. On all switch models, the DHCP server is enabled and cannot be disabled for directly connected MAPs.

The DHCP server is disabled by default for any other use.
Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — By default, all addresses except the host address of the VLAN, the network broadcast address, and the subnet broadcast address are included in the range. If you specify the range, the start address must be lower than the stop address, and all addresses must be in the same subnet. The IP interface of the VLAN must be within the same subnet but is not required to be within the range.

Examples — The following command enables the DHCP server on VLAN red-vlan to serve addresses from the 192.168.1.5 to 192.168.1.25 range:

```
WX1200# set interface red-vlan ip dhcp-server enable start
192.168.1.5 stop 192.168.1.25
success: change accepted.
```

See Also

- display dhcp-server on page 198
- set ip dns domain on page 223
- set ip dns server on page 224
Examples — The following command disables the IP interface on VLAN mauve:

WX4400# set interface mauve status down
success: set interface mauve to down

See Also
- clear interface on page 185
- display interface on page 200
- set interface on page 218

set ip alias

Configures an alias, which maps a name to an IP address. You can use aliases as shortcuts in CLI commands.

Syntax — set ip alias name ip-addr
- name — String of up to 32 alphanumeric characters, with no spaces.
- ip-addr — IP address in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command configures the alias HR1 for IP address 192.168.1.2:

WX4400# set ip alias HR1 192.168.1.2
success: change accepted.

See Also
- clear ip alias on page 186
- display ip alias on page 201
**set ip dns**

Enables or disables DNS on a wireless LAN switch.

**Syntax** — `set ip dns {enable | disable}`

- **enable** — Enables DNS.
- **disable** — Disables DNS.

**Defaults** — DNS is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command enables DNS on a WX switch:

```
WX1200# set ip dns enable
```

Start DNS Client

**See Also**

- `clear ip dns domain` on page 187
- `clear ip dns server` on page 187
- `display ip dns` on page 202
- `set ip dns domain` on page 223
- `set ip dns server` on page 224

---

**set ip dns domain**

Configures a default domain name for DNS queries. The WX appends the default domain name to domain names or hostnames you enter in commands.

**Syntax** — `set ip dns domain name`

- **name** — Domain name of between 1 and 64 alphanumeric characters with no spaces (for example, example.org).

**Defaults** — None.

**Access** — Enabled.

**Usage** — To override the default domain name when entering a hostname in a CLI command, enter a period at the end of the hostname. For example, if the default domain name is example.com, enter `chris.` if the fully qualified hostname is `chris` and not `chris.example.com.`
Aliases take precedence over DNS. When you enter a hostname, MSS checks for an alias with that name first, before using DNS to resolve the name.

**Examples** — The following command configures the default domain name example.com:

```
WX1200# set ip dns domain example.com
Domain name changed
```

**See Also**
- `clear ip dns domain` on page 187
- `clear ip dns server` on page 187
- `display ip dns` on page 202
- `set ip dns` on page 223
- `set ip dns server` on page 224

---

### set ip dns server

Specifies a DNS server to use for resolving hostnames you enter in CLI commands.

**Syntax** — `set ip dns server ip-addr {primary | secondary}`

- `ip-addr` — IP address of a DNS server, in dotted decimal or CIDR notation.
- `primary` — Makes the server the primary server, which MSS always consults first for resolving DNS queries.
- `secondary` — Makes the server a secondary server. MSS consults a secondary server only if the primary server does not reply.

**Defaults** — None.

**Access** — Enabled.

**Usage** — You can configure a WX to use one primary DNS server and up to five secondary DNS servers.

**Examples** — The following commands configure a WX to use a primary DNS server and two secondary DNS servers:

```
WX1200# set ip dns server 10.10.10.50/24 primary
success: change accepted.
```

```
WX1200# set ip dns server 10.10.20.69/24 secondary
```
success: change accepted.
WX1200# set ip dns server 10.10.30.69/24 secondary
success: change accepted.

See Also
- clear ip dns domain on page 187
- clear ip dns server on page 187
- display ip dns on page 202
- set ip dns on page 223
- set ip dns domain on page 223

### set ip https server

Enables the HTTPS server on a WX. The HTTPS server is required for Web View access to the switch.

⚠️ **CAUTION:** If you disable the HTTPS server, Web View access to the WX switch is also disabled.

**Syntax** — `set ip https server {enable | disable}`
- `enable` — Enables the HTTPS server.
- `disable` — Disables the HTTPS server.

**Defaults** — The HTTPS server is disabled by default.

**Access** — Enabled.

**History** — The default is changed to disabled in 3.1. In addition, the HTTPS server is no longer required for WebAAA.

**Examples** — The following command enables the HTTPS server on a WX switch:

WX1200# set ip https server enable
success: change accepted.

See Also
- clear ip telnet on page 189
- display ip https on page 203
- display ip telnet on page 206
- set ip telnet on page 229
- set ip telnet server on page 230
set ip route

Adds a static route to the IP route table.

**Syntax**

```plaintext
set ip route {default | ip-addr mask | ip-addr/mask-length} gateway metric
```

- **default** — Default route. A WX switch uses the default route if an explicit route is not available for the destination.

  Default is an alias for IP address 0.0.0.0/0.

- **ip-addr mask** — IP address and subnet mask for the route destination, in dotted decimal notation (for example, 10.10.10.10 255.255.255.0).

- **ip-addr/mask-length** — IP address and subnet mask length in CIDR format (for example, 10.10.10.10/24).

- **gateway** — IP address, DNS hostname, or alias of the next-hop router.

- **metric** — Cost for using the route. You can specify a value from 0 through 2,147,483,647. Lower-cost routes are preferred over higher-cost routes.

**Defaults** — The HTTPS server is enabled by default.

**Access** — Enabled.

**Usage** — MSS can use a static route only if a direct route in the route table resolves the static route. MSS adds routes with next-hop types Local and Direct when you add an IP interface to a VLAN, if the VLAN is up. If one of these added routes can resolve the static route, MSS can use the static route.

Before you add a static route, use the `display interface` command to verify that the WX switch has an IP interface in the same subnet as the route's next-hop router. If not, the VLAN:Interface field of the `display ip route` command output shows that the route is down.

You can configure a maximum of 4 routes per destination. This includes default routes, which have destination 0.0.0.0/0. Each route to a given destination must have a unique gateway address. When the route table contains multiple default or explicit routes to the same destination, MSS uses the route with the lowest cost. If two or more routes to the same destination have the lowest cost, MSS selects the first route in the route table.
When you add multiple routes to the same destination, MSS groups the routes and orders them from lowest cost at the top of the group to highest cost at the bottom of the group. If you add a new route that has the same destination and cost as a route already in the table, MSS places the new route at the top of the group of routes with the same cost.

**Examples** — The following command adds a default route that uses gateway 10.5.4.1 and gives the route a cost of 1:

```
WX4400# set ip route default 10.5.4.1 1
success: change accepted.
```

The following commands add two default routes, and configure MSS to always use the route through 10.2.4.69 when the interface to that gateway router is up:

```
WX4400# set ip route default 10.2.4.69 1
success: change accepted.
WX4400# set ip route default 10.2.4.17 2
success: change accepted.
```

The following command adds an explicit route from a WX to any host on the 192.168.4.x subnet through the local router 10.5.4.2, and gives the route a cost of 1:

```
WX4400# set ip route 192.168.4.0 255.255.255.0 10.5.4.2 1
success: change accepted.
```

The following command adds another explicit route, using CIDR notation to specify the subnet mask:

```
WX4400# set ip route 192.168.5.0/24 10.5.5.2 1
success: change accepted.
```

**See Also**

- `clear ip route` on page 188
- `display interface` on page 200
- `display ip route` on page 204
set ip snmp server

Enables or disables the SNMP service on the WX.

Syntax — set ip snmp server {enable | disable}

  enable — Enables the SNMP service.
  disable — Disables the SNMP service.

Defaults — The SNMP service is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command enables the SNMP server on a WX switch:

WX4400# set ip snmp server enable
success: change accepted.

See Also
- set port trap on page 144
- set snmp community on page 233

set ip ssh

Changes the TCP port number on which a WX listens for Secure Shell (SSH) management traffic.

CAUTION: If you change the SSH port number from an SSH session, MSS immediately ends the session. To open a new management session, you must configure the SSH client to use the new TCP port number.

Syntax — set ip ssh port port-num

  port-num — TCP port number.

Defaults — The default SSH port number is 22.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the SSH port number on a WX switch to 6000:

WX4400# set ip ssh port 6000
success: change accepted.
set ip ssh server

Disables or reenables the SSH server on a WX.

CAUTION: If you disable the SSH server, SSH access to the WX is also disabled.

Syntax — set ip ssh server {enable | disable}

- enable — Enables the SSH server.
- disable — Disables the SSH server.

Defaults — The SSH server is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must generate an SSH authentication key to use SSH.

The maximum number of SSH sessions supported on a WX is eight. If Telnet is also enabled, the WX can have up to eight Telnet or SSH sessions, in any combination, and one Console session.

See Also
- crypto generate key on page 613
- set ip ssh on page 228
- set ip ssh server on page 229

set ip telnet

Changes the TCP port number on which a WX listens for Telnet management traffic.

CAUTION: If you change the Telnet port number from a Telnet session, MSS immediately ends the session. To open a new management session, you must Telnet to the WX with the new Telnet port number.

Syntax — set ip telnet port-num

- port-num — TCP port number.
CHAPTER 7: IP SERVICES COMMANDS

Defaults — The default Telnet port number is 23.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the Telnet port number on a WX to 5000:

```
WX4400# set ip telnet 5000
success: change accepted.
```

See Also
- `clear ip telnet` on page 189
- `display ip https` on page 203
- `display ip telnet` on page 206
- `set ip https server` on page 225
- `set ip telnet server` on page 230

---

**set ip telnet server** Enables the Telnet server on a WX.

⚠️ CAUTION: If you disable the Telnet server, Telnet access to the WX is also disabled.

Syntax — `set ip telnet server {enable | disable}`
- `enable` — Enables the Telnet server.
- `disable` — Disables the Telnet server.

Defaults — The Telnet server is disabled by default.

Access — Enabled.

Usage — The maximum number of Telnet sessions supported on a WX is eight. If SSH is also enabled, the WX can have up to eight Telnet or SSH sessions, in any combination, and one console session.

Examples — The following command enables the Telnet server on a WX:

```
WX4400# set ip telnet server enable
success: change accepted.
```
set ntp

Enables or disables the NTP client on a WX.

Syntax — *set ntp {enable | disable}*

- *enable* — Enables the NTP client.
- *disable* — Disables the NTP client.

Defaults — The NTP client is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If NTP is configured on a system whose current time differs from the NTP server time by more than 10 minutes, convergence of the WX time can take many NTP update intervals. 3Com recommends that you set the time manually to the NTP server time before enabling NTP to avoid a significant delay in convergence.

Examples — The following command enables the NTP client:

```
WX4400# set ntp enable
success: NTP Client enabled
```

See Also

- *clear ntp server* on page 189
- *clear ntp update-interval* on page 190
- *display ntp* on page 207
- *set ntp server* on page 232
- *set ntp update-interval* on page 233
set ntp server

Configures a WX to use an NTP server.

**Syntax** — `set ntp server ip-addr`

- `ip-addr` — IP address of the NTP server, in dotted decimal notation.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can configure up to three NTP servers. MSS queries all the servers and selects the best response based on the method described in RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis.

To use NTP, you also must enable the NTP client with the `set ntp` command.

**Examples** — The following command configures a WX switch to use NTP server 192.168.1.5:

```
WX4400# set ntp server 192.168.1.5
```

**See Also**
- `clear ntp server` on page 189
- `clear ntp update-interval` on page 190
- `display ntp` on page 207
- `set ntp` on page 231
- `set ntp update-interval` on page 233
**set ntp update-interval**

Changes how often a WX sends queries to the NTP servers for updates.

**Syntax** — `set ntp update-interval seconds`

- `seconds` — Number of seconds between queries. You can specify from 16 through 1,024 seconds.

**Defaults** — The default NTP update interval is 64 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command changes the NTP update interval to 128 seconds:

```
WX4400# set ntp update-interval 128
success: change accepted.
```

**See Also**

- clear ntp server on page 189
- clear ntp update-interval on page 190
- display ntp on page 207
- set ntp on page 231
- set ntp server on page 232

**set snmp community**

Configures a community string for SNMPv1 or SNMPv2c.

For SNMPv3, use the `set snmp usm` command to configure an SNMPv3 user. SNMPv3 does not use community strings.

**Syntax** — `set snmp community comm-string access {read-only | read-notify | notify-only | read-write | notify-read-write}`

- `comm-string` — Name of the SNMP community. Specify between 1 and 32 alphanumeric characters, with no spaces.
- `read-only` — Allows an SNMP management application using the string to get (read) object values on the switch but not to set (write) them.
- **read-notify** — Allows an SNMP management application using the string to get object values on the switch but not to set them. The switch can use the string to send notifications.

- **notify-only** — Allows the WX to use the string to send notifications.

- **read-write** — Allows an SNMP management application using the string to get and set object values on the switch.

- **notify-read-write** — Allows an SNMP management application using the string to get and set object values on the switch. The switch also can use the string to send notifications.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Default community strings changed from `public` (for read-only) and `private` (for read-write) to blank in MSS Version 3.1. Default strings removed and new access types added for SNMPv3 (read-notify, notify-only, notify-read-write) in MSS Version 4.0.

**Usage** — SNMP community strings are passed as clear text in SNMPv1 and SNMPv2c. 3Com recommends that you use strings that cannot easily be guessed by unauthorized users. For example, do not use the well-known strings `public` and `private`.

If you are using SNMPv3, you can configure SNMPv3 users to use authentication and to encrypt SNMP data.

**Examples** — The following command configures the read-write community `good_community`:

```
WX4400# set snmp community read-write good_community
success: change accepted.
```

The following command configures community string `switchmgr1` with access level notify-read-write:

```
WX4400# set snmp community name switchmgr1 notify-read-write
success: change accepted.
```
set snmp notify profile

Configures an SNMP notification profile. A notification profile is a named list of all the notification types that can be generated by a switch, and for each notification type, the action to take (drop or send) when an event occurs.

You can configure up to ten notification profiles.

**Syntax** — `set snmp notify profile {default | profile-name} {drop | send} {notification-type | all}`

- **default | profile-name** — Name of the notification profile you are creating or modifying. The profile-name can be up to 32 alphanumeric characters long, with no spaces. To modify the default notification profile, specify `default`.
- **drop | send** — Specifies the action that the SNMP engine takes with regard to the notifications you specify with notification-type or all.
- **notification-type** — Name of the notification type:
  - **APBootTraps**—Generated when a MAP access point boots.
  - **ApNonOperStatusTraps**—Generated to indicate a MAP radio is nonoperational.
  - **ApOperRadioStatusTraps**—Generated when the status of a MAP radio changes.
  - **APRejectLicenseExceededTraps**—Generated when a WX switch receives a packet from an inactive AP and attaching that AP would make the WX switch exceed the maximum (licensed) number of active APs.

See Also

- **clear snmp community** on page 191
- **set ip snmp server** on page 228
- **set snmp notify target** on page 240
- **set snmp notify profile** on page 235
- **set snmp protocol** on page 245
- **set snmp security** on page 246
- **set snmp usm** on page 247
- **display snmp community** on page 209
- **APTimeoutTraps**—Generated when a MAP access point fails to respond to the WX switch.
- **AuthenTraps**—Generated when the WX switch’s SNMP engine receives a bad community string.
- **AutoTuneRadioChannelChangeTraps**—Generated when the RF Auto-Tuning feature changes the channel on a radio.
- **AutoTuneRadioPowerChangeTraps**—Generated when the RF Auto-Tuning feature changes the power setting on a radio.
- **ClientAssociationFailureTraps**—Generated when a client’s attempt to associate with a radio fails.
- **ClientAssociationSuccessTraps**—Generated when a client is successfully associated.
- **ClientAuthorizationSuccessTraps**—Generated when a client is successfully authorized.
- **ClientAuthenticationFailureTraps**—Generated when authentication fails for a client.
- **ClientAuthenticationSuccessTraps**—Generated when a client is successfully authenticated.
- **ClientAuthorizationFailureTraps**—Generated when authorization fails for a client.
- **ClientClearedTraps**—Generated when a client’s session is cleared.
- **ClientDeAssociationTraps**—Generated when a client is dissociated from a radio.
- **ClientDeAuthenticationTraps**—Generated when a client is disauthenticated from a radio.
- **ClientDot1xFailureTraps**—Generated when a client experiences an 802.1X failure.
- **ClientIpAddressChangeTraps**—Generated when a client’s IP address changes.
- **ClientRoamingTraps**—Generated when a client roams.
- **CounterMeasureStartTraps**—Generated when MSS begins countermeasures against a rogue access point.
- **CounterMeasureStopTraps**—Generated when MSS stops countermeasures against a rogue access point.
DAPConnectWarningTraps—Generated when a Distributed MAP whose fingerprint has not been configured in MSS establishes a management session with the switch.

DeviceFailTraps—Generated when an event with an Alert severity occurs.

DeviceOkayTraps—Generated when a device returns to its normal state.

LinkDownTraps—Generated when the link is lost on a port.

LinkUpTraps—Generated when the link is detected on a port.

MichaelMICFailureTraps—Generated when two Michael message integrity code (MIC) failures occur within 60 seconds, triggering Wi-Fi Protected Access (WPA) countermeasures.

MobilityDomainJoinTraps—Generated when the WX switch is initially able to contact a mobility domain seed member, or can contact the seed member after a timeout.

MobilityDomainTimeoutTraps—Generated when a timeout occurs after a WX switch has unsuccessfully tried to communicate with a seed member.

PoEFailTraps—Generated when a serious PoE problem, such as a short circuit, occurs.

RFDetectAdhocUserTraps—Generated when MSS detects an ad-hoc user.

RFDetectAdhocUserDisappearTraps—Generated when an ad-hoc user is no longer being detected.

RFDetectBlacklistedTraps—Generated when an association, re-association, or deassociation request is detected from a blacklisted transmitter.

RFDetectRogueAPTraps—Generated when MSS detects a rogue access point.

RFDetectRogueDisappearTraps—Generated when a rogue access point is no longer being detected.

RFDetectClientViaRogueWiredAPTraps—Generated when MSS detects, on the wired part of the network, the MAC address of a wireless client associated with a third-party AP.
- **RFDetectDoSPortTraps**—Generated when MSS detects an associate request flood, reassociate request flood, or disassociate request flood.

- **RFDetectDoSTraps**—Generated when MSS detects a DoS attack other than an associate request flood, reassociate request flood, or disassociate request flood.

- **RFDetectInterferingRogueAPTraps**—Generated when an interfering device is detected.

- **RFDetectInterferingRogueDisappearTraps**—Generated when an interfering device is no longer detected.

- **RFDetectSpoofedMacAPTraps**—Generated when MSS detects a wireless packet with the source MAC address of a MAP, but without the spoofed MAP's signature (fingerprint).

- **RFDetectSpoofedSsidAPTraps**—Generated when MSS detects beacon frames for a valid SSID, but sent by a rogue AP.

- **RFDetectUnAuthorizedAPTraps**—Generated when MSS detects the MAC address of a MAP that is on the attack list.

- **RFDetectUnAuthorizedOuiTraps**—Generated when a wireless device that is not on the list of permitted vendors is detected.

- **RFDetectUnAuthorizedSsidTraps**—Generated when an SSID that is not on the permitted SSID list is detected.

- **all**—Sends or drops all notifications.

**Defaults**—A default notification profile (named *default*) is already configured on the WX. All notifications in the default profile are dropped by default.

**Access**—Enabled.

**History**—Introduced in MSS Version 4.0.

**Examples**—The following command changes the action in the default notification profile from *drop* to *send* for all notification types:

```
WX1200# set snmp notify profile default send all
success: change accepted.
```

The following commands create notification profile *snmpprof_rfdetect*, and change the action to *send* for all RF detection notification types:
set snmp notify profile

WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserDisappearTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectBlacklistedUserTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectClientViaRogueWiredAPTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectDoSTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectAdhocUserTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectInterferingRogueAPTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectInterferingRogueDisappearTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectRogueAPTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectRogueDisappearTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectSpoofedMacAPTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectSpoofedSsidAPTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectUnauthorizedAPTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectUnauthorizedOuiTraps
  success: change accepted.
WX1200# set snmp notify profile snmpprof_rfdetect send RFDetectUnauthorizedSsidTraps
  success: change accepted.
set snmp notify target

Configures a notification target for notifications from SNMP.

A notification target is a remote device that the WX sends SNMP notifications. You can configure the MSS SNMP engine to send confirmed notifications (informs) or unconfirmed notifications (traps). Some of the command options differ depending on the SNMP version and the type of notification you specify. You can configure up to 10 notification targets.

SNMPv3 with Informs

To configure a notification target for informs from SNMPv3, use the following command:

**Syntax** — set snmp notify target target-num
ip-addr[:udp-port-number]
usm inform user username
snmp-engine-id {ip | hex hex-string}
[profile profile-name]
[security {unsecured | authenticated | encrypted}]
[retries num]
[timeout num]

- **target-num** — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- **ip-addr[:udp-port-number]** — IP address of the server. You also can specify the UDP port number to send notifications to.
username — USM username. This option is applicable only when the SNMP version is usm. If the user will send informs rather than traps, you also must specify the snmp-engine-id of the target.

snmp-engine-id — SNMP engine ID of the target. Specify ip if the target SNMP engine ID is based on its IP address. If the target’s SNMP engine ID is a hexadecimal value, use hex hex-string to specify the value.

profile profile-name — Notification profile that this SNMP user will use to specify the notification types to send or drop.

security — Specifies the security level, and is applicable only when the SNMP version is usm:

- unsecured — Message exchanges are not authenticated, nor are they encrypted. This is the default.
- authenticated — Message exchanges are authenticated, but are not encrypted.
- encrypted — Message exchanges are authenticated and encrypted.

retries num — Specifies the number of times the MSS SNMP engine will resend a notification that has not been acknowledged by the target. You can specify from 0 to 3 retries.

timeout num — Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.

SNMPv3 with Traps

To configure a notification target for traps from SNMPv3, use the following command:

Syntax — set snmp notify target target-num ip-addr[:udp-port-number] usm trap user username [profile profile-name] [security {unsecured | authenticated | encrypted}]

- target-num — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- ip-addr[:udp-port-number] — IP address of the server. You also can specify the UDP port number to send notifications to.
- **username** — USM username. This option is applicable only when the SNMP version is **usm**.

- **profile profile-name** — Notification profile this SNMP user will use to specify the notification types to send or drop.

- **security** — Specifies the security level, and is applicable only when the SNMP version is **usm**:
  - **unsecured** — Message exchanges are not authenticated, nor are they encrypted. This is the default.
  - **authenticated** — Message exchanges are authenticated, but are not encrypted.
  - **encrypted** — Message exchanges are authenticated and encrypted.

---

**SNMPv2c with Informs**

To configure a notification target for informs from SNMPv2c, use the following command:

**Syntax** — set snmp notify target target-num ip-addr[:udp-port-number] v2c community-string inform [profile profile-name] [retries num] [timeout num]

- **target-num** — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.

- **ip-addr[:udp-port-number]** — IP address of the server. You also can specify the UDP port number to send notifications to.

- **community-string** — Community string.

- **profile profile-name** — Notification profile this SNMP user will use to specify the notification types to send or drop.

- **retries num** — Notification profile this SNMP user will use to specify the notification types to send or drop.

- **timeout num** — Specifies the number of seconds MSS waits for acknowledgement of a notification. You can specify from 1 to 5 seconds.
**SNMPv2c with Traps**

To configure a notification target for traps from SNMPv2c, use the following command:

**Syntax** — set snmp notify target target-num ip-addr[:udp-port-number] v2c community-string trap [profile profile-name]

- **target-num** — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- **ip-addr[:udp-port-number]** — IP address of the server. You also can specify the UDP port number to send notifications to.
- **community-string** — Community string.
- **profile profile-name** — Notification profile this SNMP user will use to specify the notification types to send or drop.

**SNMPv1 with Traps**

To configure a notification target for traps from SNMPv1, use the following command:

**Syntax** — set snmp notify target target-num ip-addr[:udp-port-number] v1 community-string [profile profile-name]

- **target-num** — ID for the target. This ID is local to the WX switch and does not need to correspond to a value on the target itself. You can specify a number from 1 to 10.
- **ip-addr[:udp-port-number]** — IP address of the server. You also can specify the UDP port number to send notifications to.
- **community-string** — Community string.
- **profile profile-name** — Notification profile this SNMP user will use to specify the notification types to send or drop.

**Defaults** — The default UDP port number on the target is 162. The default minimum required security level is **unsecured**. The default number of retries is 0 and the default timeout is 2 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.
Usage — The inform or trap option specifies whether the MSS SNMP engine expects the target to acknowledge notifications sent to the target by the WX switch. Use inform if you want acknowledgements. Use trap if you do not want acknowledgements. The inform option is applicable to SNMP version v2c or usm only.

Examples — The following command configures a notification target for acknowledged notifications:

```plaintext
WX1200# set snmp notify target 1 10.10.40.9 usm inform user
    securesnmpmgr1 snmp-engine-id ip
success: change accepted.
```

This command configures target 1 at IP address 10.10.40.9. The target's SNMP engine ID is based on its address. The MSS SNMP engine will send notifications based on the default profile, and will require the target to acknowledge receiving them.

The following command configures a notification target for unacknowledged notifications:

```plaintext
WX1200# set snmp notify target 2 10.10.40.10 v1 trap
success: change accepted.
```

See Also

- `clear snmp notify target` on page 192
- `set ip snmp server` on page 228
- `set snmp community` on page 233
- `set snmp notify profile` on page 235
- `set snmp protocol` on page 245
- `set snmp security` on page 246
- `set snmp usm` on page 247
- `display snmp notify target` on page 210
**set snmp protocol**

Enables an SNMP protocol. MSS supports SNMPv1, SNMPv2c, and SNMPv3.

**Syntax** — `set snmp protocol {v1 | v2c | usm | all} {enable | disable}`

- **v1** — SNMPv1
- **v2c** — SNMPv2c
- **usm** — SNMPv3 (with the user security model)
- **all** — Enables all supported versions of SNMP.
- **enable** — Enables the specified SNMP version(s).
- **disable** — Disables the specified SNMP version(s).

**Defaults** — All SNMP versions are disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — SNMP requires the switch system IP address to be set. SNMP does not work without the system IP address.

You also must enable the SNMP service using the `set ip snmp server` command.

**Examples** — The following command enables all SNMP versions:

```bash
WX1200# set snmp protocol all enable
success: change accepted.
```

**See Also**

- `set ip snmp server` on page 228
- `set snmp community` on page 233
- `set snmp notify target` on page 240
- `set snmp security` on page 246
- `set snmp usm` on page 247
- `display snmp status` on page 211
**set snmp security**

Sets the minimum level of security MSS requires for SNMP message exchanges.

**Syntax**

```
set snmp security
{unsecured | authenticated | encrypted | auth-req-unsec-notify}
```

- **unsecured** — SNMP message exchanges are not secure. This is the only value supported for SNMPv1 and SNMPv2c.
- **authenticated** — SNMP message exchanges are authenticated but are not encrypted.
- **encrypted** — SNMP message exchanges are authenticated and encrypted.
- **auth-req-unsec-notify** — SNMP message exchanges are authenticated but are not encrypted, and notifications are neither authenticated nor encrypted.

**Defaults** — By default, MSS allows nonsecure (**unsecured**) SNMP message exchanges.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — SNMPv1 and SNMPv2c do not support authentication or encryption. If you plan to use SNMPv1 or SNMPv2c, leave the minimum level of SNMP security set to **unsecured**.

**Examples** — The following command sets the minimum level of SNMP security allowed to authentication and encryption:

```
WX1200# set snmp security encrypted
success: change accepted.
```

**See Also**

- **set ip snmp server** on page 228
- **set snmp community** on page 233
- **set snmp notify target** on page 240
- **set snmp notify profile** on page 235
- **set snmp protocol** on page 245
set snmp usm

This command does not apply to SNMPv1 or SNMPv2c. For these SNMP versions, use the set snmp community command to configure community strings.

Syntax — set snmp usm usm-username
snmp-engine-id {ip ip-addr | local | hex hex-string}
access {read-only | read-notify | notify-only | read-write | notify-read-write}
auth-type {none | md5 | sha} {auth-pass-phrase string | auth-key hex-string}
encrypt-type {none | des | 3des | aes} {encrypt-pass-phrase string | encrypt-key hex-string}

- **usm-username** — Name of the SNMPv3 user. Specify between 1 and 32 alphanumeric characters, with no spaces.
- **snmp-engine-id {ip ip-addr | local | hex hex-string}** — Specifies a unique identifier for the SNMP engine. To send informs, you must specify the engine ID of the inform receiver. To send traps and to allow get and set operations and so on, specify local as the engine ID.
- **hex hex-string** — ID is a hexadecimal string.
- **ip ip-addr** — ID is based on the IP address of the station running the management application. Enter the IP address of the station. MSS calculates the engine ID based on the address.
- **local** — Uses the value computed from the switch’s system IP address.
- **access {read-only | read-notify | notify-only | read-write | notify-read-write}** — Specifies the access level of the user:
  - **read-only** — An SNMP management application using the string can get (read) object values on the switch but cannot set (write) them.
  - **read-notify** — An SNMP management application using the string can get object values on the switch but cannot set them. The switch can use the string to send notifications.
notify-only—The switch can use the string to send notifications.

read-write—An SNMP management application using the string can get and set object values on the switch.

notify-read-write — An SNMP management application using the string can get and set object values on the switch. The switch can use the string to send notifications.

auth-type {none | md5 | sha} {auth-pass-phrase string | auth-key hex-string} — Specifies the authentication type used to authenticate communications with the remote SNMP engine. You can specify one of the following:

- none—No authentication is used.
- md5—Message-digest algorithm 5 is used.
- sha—Secure Hashing Algorithm (SHA) is used.

If the authentication type is md5 or sha, you can specify a passphrase or a hexadecimal key.

- To specify a passphrase, use the auth-pass-phrase string option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
- To specify a key, use the auth-key hex-string option.

encrypt-type {none | des | 3des | aes} {encrypt-pass-phrase string | encrypt-key hex-string} — Specifies the encryption type used for SNMP traffic. You can specify one of the following:

- none—No encryption is used. This is the default.
- des—Data Encryption Standard (DES) encryption is used.
- 3des—Triple DES encryption is used.
- aes—Advanced Encryption Standard (AES) encryption is used.

If the encryption type is des, 3des, or aes, you can specify a passphrase or a hexadecimal key.

- To specify a passphrase, use the encrypt-pass-phrase string option. The string can be from 8 to 32 alphanumeric characters long, with no spaces.
- To specify a key, use the encrypt-key hex-string option.
Defaults — No SNMPv3 users are configured by default. When you configure an SNMPv3 user, the default access is read-only, and the default authentication and encryption types are both none.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command creates USM user snmpmgr1, associated with the local SNMP engine ID. This user can send traps to notification receivers.

 WX#1200  set snmp usm snmpmgr1 snmp-engine-id local
success: change accepted.

The following command creates USM user securesnmpmgr1, which uses SHA authentication and 3DES encryption with passphrases. This user can send informs to the notification receiver that has engine ID 192.168.40.2.

 WX4400#  set snmp usm securesnmpmgr1 snmp-engine-id ip
192.168.40.2 auth-type sha auth-pass-phrase myauthpword
encrypt-type 3des encrypt-pass-phrase mycryptpword
success: change accepted.

See Also

- clear snmp usm on page 192
- set ip snmp server on page 228
- set snmp community on page 233
- set snmp notify target on page 240
- set snmp notify profile on page 235
- set snmp protocol on page 245
- set snmp security on page 246
- display snmp usm on page 212
**set summertime**

Offsets the real-time clock of a WX by +1 hour and returns it to standard time for daylight savings time or a similar summertime period.

**Syntax** — `set summertime summer-name [start week weekday month hour min end week weekday month hour min]`

- **summer-name** — Name of up to 32 alphanumeric characters that describes the summertime offset. You can use a standard name or any name you like.
- **start** — Start of the time change period.
- **week** — Week of the month to start or end the time change. Valid values are first, second, third, fourth, or last.
- **weekday** — Day of the week to start or end the time change. Valid values are sun, mon, tue, wed, thu, fri, and sat.
- **month** — Month of the year to start or end the time change. Valid values are jan, feb, mar, apr, may, jun, jul, aug, sep, oct, nov, and dec.
- **hour** — Hour to start or end the time change — a value between 0 and 23 on the 24-hour clock.
- **min** — Minute to start or end the time change — a value between 0 and 59.
- **end** — End of the time change period.

**Defaults** — If you do not specify a start and end time, the system implements the time change starting at 2:00 a.m. on the first Sunday in April and ending at 2:00 a.m. on the last Sunday in October, according to the North American standard.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You must first set the time zone with the `set timezone` command for the offset to work properly without the `start` and `end` values.

Configure summertime before you set the time and date. Otherwise, summertime's adjustment of the time will make the time incorrect, if the date is within the summertime period.
Examples — To enable summertime and set the summertime time zone to PDT (Pacific Daylight Time), type the following command:

```
WX1200# set summertime PDT
success: change accepted
```

See Also
- clear summertime on page 193
- clear timezone on page 194
- display summertime on page 212
- display timedate on page 213
- display timezone on page 213
- set timedate on page 252
- set timezone on page 253

**set system ip-address**

Configures the system IP address. The system IP address determines the interface or source IP address MSS uses for system tasks, including the following:
- Mobility domain operations
- Topology reporting for dual-homed MAP access points
- Default source IP address used in unsolicited communications such as AAA accounting reports and SNMP traps

**Syntax** — `set system ip-address ip-addr`

- **ip-addr** — IP address, in dotted decimal notation. The address must be configured on one of the WX VLANs.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You must use an address that is configured on one of the WX switch VLANs.

To display the system IP address, use the *display system* command.
**Examples** — The following commands configure an IP interface on VLAN taupe and configure the interface to be the system IP address:

```
WX4400# set interface taupe ip 10.10.20.20/24
success: set ip address 10.10.20.20 netmask 255.255.255.0 on vlan taupe
WX4400# set system ip-address 10.10.20.20
success: change accepted.
```

**See Also**
- [clear system ip-address](#) on page 194
- [display system](#) on page 95
- [set interface](#) on page 218

---

**set timedate**

Sets the time of day and date on the WX.

**Syntax** — `set timedate {date mmm dd yyyy [time hh:mm:ss]}`

- `date mmm dd yyyy` — System date:
  - `mmm` — month
  - `dd` — day
  - `yyyy` — year
- `time hh:mm:ss` — System time, in hours, minutes, and seconds.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — The day of week is automatically calculated from the day that you set. The time displayed by the CLI after you type the command might be slightly later than the time you enter due to the interval between when you press Enter and when the CLI reads and displays the new time and date.

Configure summertime before you set the time and date. Otherwise, the summertime adjustment makes the time incorrect, if the date is within the summertime period.
set timezone 253

Examples — The following command sets the date to March 13, 2003 and time to 11:11:12:

WX4400# set timedate date feb 29 2004 time 23:58:00
Time now is:       Sun Feb 29 2004, 23:58:02 PST

See Also
- clear summertime on page 193
- clear timezone on page 194
- display summertime on page 212
- display timedate on page 213
- display timezone on page 213
- set summertime on page 250
- set timezone on page 253

set timezone

Sets the number of hours, and optionally the number of minutes, that the WX real-time clock is offset from Coordinated Universal Time (UTC). These values are also used by Network Time Protocol (NTP), if it is enabled.

Syntax — set timezone zone-name [-hours [minutes]]
- zone-name — Time zone name of up to 32 alphabetic characters. You can use a standard name or any name you like.
- - (minus sign) — Minus time to indicate hours (and minutes) to be subtracted from UTC. Otherwise, hours and minutes are added by default.
- hours — Number of hours to add or subtract from UTC.
- minutes — Number of minutes to add or subtract from UTC.

Defaults — If this command is not used, then the default time zone is UTC.

Access — Enabled.

History — Introduced in MSS Version 3.0.
Examples — To set the time zone for Pacific Standard Time (PST), type the following command:

WX1200# set timezone PST -8
Timezone is set to 'PST', offset from UTC is -8:0 hours.

See Also
- clear summertime on page 193
- clear timezone on page 194
- display summertime on page 212
- display timedate on page 213
- display timezone on page 213
- set summertime on page 250
- set timedate on page 252

telnet
Opens a Telnet client session with a remote device.

Syntax — telnet {ip-addr | hostname} [port port-num]
- ip-addr — IP address of the remote device.
- hostname — Hostname of the remote device.
- port port-num — TCP port number on which the TCP server on the remote device listens for Telnet connections.

Defaults — MSS attempts to establish Telnet connections with TCP port 23 by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To end a Telnet session from the remote device, press Ctrl+t or type quit or logout in the management session on the remote device. To end a client session from the local WX switch, use the clear sessions telnet client command.

If the configuration of the WX switch from which you enter the telnet command has an ACL that denies Telnet client traffic, the ACL also denies access by the telnet command.
Examples — In the following example, an administrator establishes a Telnet session with another device and enters a command on the remote device:

WX4400# telnet 10.10.10.90
Session 0 pty tty2.d Trying 10.10.10.90...
Connected to 10.10.10.90
Disconnect character is '^^t'

Copyright (c) 2004 3Com Corporation. All rights reserved.

Username: username
Password: password
WX1200-remote> display vlan

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Admin</th>
<th>VLAN</th>
<th>Tunl</th>
<th>Status</th>
<th>State</th>
<th>Affin</th>
<th>Port</th>
<th>Tag</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 default</td>
<td>Up</td>
<td>Up</td>
<td>5</td>
<td>Up</td>
<td>Up</td>
<td>3</td>
<td>none</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>3 red</td>
<td>Up</td>
<td>Up</td>
<td>5</td>
<td>Up</td>
<td>Up</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>10 backbone</td>
<td>Up</td>
<td>Up</td>
<td>5</td>
<td>Up</td>
<td>Up</td>
<td>2</td>
<td>none</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>4094 web-aaa</td>
<td>Up</td>
<td>Up</td>
<td>0</td>
<td>Up</td>
<td>Up</td>
<td>2</td>
<td>4094</td>
<td>Up</td>
<td></td>
</tr>
</tbody>
</table>

When the administrator presses Ctrl+t to end the Telnet connection, the management session returns to the local prompt:

WX1200-remote> Session 0 pty tty2.d terminated tt name tty2.d
WX1200#

See Also

- clear sessions on page 661
- display sessions on page 664

traceroute

Traces the route to an IP host.

Syntax — traceroute host [dnf] [no-dns] [port port-num] [queries num] [size size] [ttl hops] [wait ms]

- host — IP address, hostname, or alias of the destination host. Specify the IP address in dotted decimal notation.
• **dnf** — Sets the Do Not Fragment bit in the ping packet to prevent the packet from being fragmented.

• **no-dns** — Prevents MSS from performing a DNS lookup for each hop to the destination host.

• **port** `port-num` — TCP port number listening for the traceroute probes.

• **queries** `num` — Number of probes per hop.

• **size** `size` — Probe packet size in bytes. You can specify from 40 through 1,460.

• **ttl** `hops` — Maximum number of hops, which can be from 1 through 255.

• **wait** `ms` — Probe wait in milliseconds. You can specify from 1 through 100,000.

**Defaults**

• **dnf** — Disabled

• **no-dns** — Disabled

• **port** — 33434

• **queries** — 3

• **size** — 38

• **ttl** — 30

• **wait** — 5000

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Usage** — To stop a traceroute command that is in progress, press Ctrl+C.

**Examples** — The following example traces the route to host server1:

```
WX4400# traceroute server1
traceroute to server1.example.com (192.168.22.7), 30 hops max, 38 byte packets
1 engineering-1.example.com (192.168.192.206) 2 ms 1 ms 1 ms
2 engineering-2.example.com (192.168.196.204) 2 ms 3 ms 2 ms
3 gateway_a.example.com (192.168.1.201) 6 ms 3 ms 3 ms
4 server1.example.com (192.168.22.7) 3 ms * 2 ms
```
The first row of the display indicates the target host, the maximum number of hops, and the packet size. Each numbered row displays information about one hop. The rows are displayed in the order in which the hops occur, beginning with the hop closest to the WX switch.

The row for a hop lists the total time in milliseconds for each ICMP packet to reach the router or host, plus the time for the ICMP Time Exceeded message to return to the host.

An exclamation point (!) following any of these values indicates that the Port Unreachable message returned by the destination has a maximum hop count of 0 or 1. This can occur if the destination uses the maximum hop count value from the arriving packet as the maximum hop count in its ICMP reply. The reply does not arrive at the source until the destination receives a traceroute packet with a maximum hop count equal to the number of hops between the source and destination.

An asterisk (*) indicates that the timeout period expired before MSS received a Time Exceeded message for the packet.

If Traceroute receives an ICMP error message other than a Time Exceeded or Port Unreachable message, MSS displays one of the error codes described in Table 41 instead of displaying the round-trip time or an asterisk (*).

Table 41 describes the traceroute error messages.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!N</td>
<td>No route to host. The network is unreachable.</td>
</tr>
<tr>
<td>!H</td>
<td>No route to host. The host is unreachable.</td>
</tr>
<tr>
<td>!P</td>
<td>Connection refused. The protocol is unreachable.</td>
</tr>
<tr>
<td>!F</td>
<td>Fragmentation needed but Do Not Fragment (DNF) bit was set.</td>
</tr>
<tr>
<td>!S</td>
<td>Source route failed.</td>
</tr>
<tr>
<td>!A</td>
<td>Communication administratively prohibited.</td>
</tr>
<tr>
<td>7</td>
<td>Unknown error occurred.</td>
</tr>
</tbody>
</table>

See Also
- ping on page 214
Use authentication, authorization, and accounting (AAA) commands to provide a secure network connection and a record of user activity. Location policy commands override any virtual LAN (VLAN) or security ACL assignment by AAA or the local WX database to help you control access locally.

(Security ACLs are packet filters. For command descriptions, see Chapter 14.)

### Commands by Usage

This chapter presents AAA commands alphabetically. Use Table 42 to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>set authentication console on page 289</td>
</tr>
<tr>
<td></td>
<td>set authentication admin on page 287</td>
</tr>
<tr>
<td></td>
<td>set authentication dot1x on page 291</td>
</tr>
<tr>
<td></td>
<td>set authentication mac on page 295</td>
</tr>
<tr>
<td></td>
<td>set authentication proxy on page 301</td>
</tr>
<tr>
<td></td>
<td>clear authentication admin on page 262</td>
</tr>
<tr>
<td></td>
<td>clear authentication console on page 263</td>
</tr>
<tr>
<td></td>
<td>clear authentication dot1x on page 264</td>
</tr>
<tr>
<td></td>
<td>clear authentication mac on page 265</td>
</tr>
<tr>
<td></td>
<td>clear authentication proxy on page 266</td>
</tr>
<tr>
<td></td>
<td>clear authentication web on page 266</td>
</tr>
</tbody>
</table>
Table 42  AAA Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Authorization</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>for Password Users</td>
<td>set user</td>
<td>319</td>
</tr>
<tr>
<td></td>
<td>clear user</td>
<td>272</td>
</tr>
<tr>
<td></td>
<td>set user attr</td>
<td>321</td>
</tr>
<tr>
<td></td>
<td>clear user attr</td>
<td>273</td>
</tr>
<tr>
<td></td>
<td>set usergroup</td>
<td>323</td>
</tr>
<tr>
<td></td>
<td>clear usergroup</td>
<td>275</td>
</tr>
<tr>
<td></td>
<td>set user group</td>
<td>323</td>
</tr>
<tr>
<td></td>
<td>clear user group</td>
<td>274</td>
</tr>
<tr>
<td></td>
<td>clear usergroup attr</td>
<td>276</td>
</tr>
<tr>
<td>for MAC Users</td>
<td>set mac-user</td>
<td>308</td>
</tr>
<tr>
<td></td>
<td>clear mac-user</td>
<td>268</td>
</tr>
<tr>
<td></td>
<td>set mac-user attr</td>
<td>309</td>
</tr>
<tr>
<td></td>
<td>clear mac-user attr</td>
<td>269</td>
</tr>
<tr>
<td></td>
<td>set mac-usergroup attr</td>
<td>315</td>
</tr>
<tr>
<td></td>
<td>clear mac-usergroup attr</td>
<td>271</td>
</tr>
<tr>
<td></td>
<td>clear mac-user group</td>
<td>269</td>
</tr>
<tr>
<td></td>
<td>clear mac-usergroup</td>
<td>270</td>
</tr>
<tr>
<td>Accounting</td>
<td>set web-portal</td>
<td>326</td>
</tr>
<tr>
<td>Accounting</td>
<td>set accounting (admin</td>
<td>console)</td>
</tr>
<tr>
<td></td>
<td>set accounting (dot1x</td>
<td>mac</td>
</tr>
<tr>
<td></td>
<td>display accounting statistics</td>
<td>280</td>
</tr>
<tr>
<td></td>
<td>clear accounting</td>
<td>261</td>
</tr>
<tr>
<td>AAA information</td>
<td>display aaa</td>
<td>277</td>
</tr>
<tr>
<td>Mobility Profiles</td>
<td>set mobility-profile</td>
<td>317</td>
</tr>
<tr>
<td></td>
<td>set mobility-profile mode</td>
<td>319</td>
</tr>
<tr>
<td></td>
<td>display mobility-profile</td>
<td>283</td>
</tr>
<tr>
<td></td>
<td>clear mobility-profile</td>
<td>272</td>
</tr>
<tr>
<td>Location Policy</td>
<td>set location policy</td>
<td>304</td>
</tr>
<tr>
<td></td>
<td>display location policy</td>
<td>282</td>
</tr>
<tr>
<td></td>
<td>clear location policy</td>
<td>267</td>
</tr>
</tbody>
</table>
clear accounting

Removes accounting services for specified wireless users with administrative access or network access.

**Syntax** — `clear accounting {admin | dot1x} {user-glob}`

- **admin** — Users with administrative access to the WX through a console connection or through a Telnet or Web View connection.
- **dot1x** — Users with network access through the WX. Users with network access are authorized to use the network through either an IEEE 802.1X method or their media access control (MAC) address.
- **user-glob** — Single user or set of users with administrative access or network access.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
Examples — The following command removes accounting services for authorized network user Nin:

```
WX4400# clear accounting dot1x Nin
success: change accepted.
```

See Also

- `set accounting {admin | console}` on page 283
- `display accounting statistics` on page 280

---

clear authentication admin

Removes an authentication rule for administrative access through Telnet or Web Manager.

**Syntax** — `clear authentication admin user-glob`

- `user-glob` — A single user or set of users.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

*The syntax descriptions for the clear authentication commands are separate for clarity. However, the options and behavior for the clear authentication admin command are the same as in previous releases.*

**Examples** — The following command clears authentication for administrator Jose:

```
WX4400# clear authentication admin Jose
success: change accepted.
```

**See Also**

- `clear authentication console` on page 263
- `clear authentication dot1x` on page 264
clear authentication console

Removes an authentication rule for administrative access through the Console.

Syntax — clear authentication console user-glob

- user-glob — A single user or set of users.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears authentication for administrator Regina:

```
WX4400# clear authentication console Regina
success: change accepted.
```

See Also

- clear authentication admin on page 262
- display aaa on page 277
- clear authentication dot1x on page 264
- clear authentication mac on page 265
clear authentication dot1x

Removes an 802.1X authentication rule.

**Syntax** — `clear authentication dot1x {ssid ssid-name | wired} user-glob`

- `ssid ssid-name` — SSID name to which this authentication rule applies.
- `wired` — Clears a rule used for access over a WX wired-authentication port.
- `user-glob` — A single user or a set of users with 802.1X network access.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command removes 802.1X authentication for network users with usernames ending in @thiscorp.com who try to access SSID finance:

```
WX4400# clear authentication dot1x ssid finance *@thiscorp.com
```

**See Also**

- `clear authentication admin` on page 262
- `clear authentication console` on page 263
- `clear authentication mac` on page 265
- `clear authentication mac` on page 265
clear authentication mac

Removes a MAC authentication rule.

Syntax — clear authentication mac {ssid ssid-name | wired} mac-addr-glob
- ssid ssid-name — SSID name to apply the authentication.
- wired — Clears a rule used for access over a WX wired-authentication port.
- mac-addr-glob — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 79.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes a MAC authentication rule for access to SSID thatcorp by MAC addresses beginning with aa:bb:cc:

WX4400# clear authentication mac ssid thatcorp aa:bb:cc:*

See Also
- clear authentication admin on page 262
- clear authentication console on page 263
- clear authentication dot1x on page 264
- clear authentication mac on page 265
- clear authentication proxy on page 266
- display aaa on page 277
- set authentication mac on page 295
clear authentication proxy

Removes a proxy rule for third-party AP users.

**Syntax**

```bash
— clear authentication proxy ssid ssid-name user-glob
```

- `ssid ssid-name` — SSID name to which this authentication rule applies.
- `user-glob` — User-glob associated with the rule you are removing.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command removes the proxy rule for SSID `mycorp` and userglob `**`:

```bash
WX4400# clear authentication proxy ssid mycorp
```

**See Also**

- `set authentication proxy` on page 301
- `display aaa` on page 277

---

clear authentication web

Removes a WebAAA rule.

**Syntax**

```bash
— clear authentication web {ssid ssid-name | wired} user-glob
```

- `ssid ssid-name` — SSID name to which this authentication rule applies.
- `wired` — Clears a rule used for access over a WX switch's wired-authentication port.
- `user-glob` — User-glob associated with the rule you are removing.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 3.0.
clear location policy

Examples — The following command removes WebAAA for SSID research and userglob temp*@thiscorp.com:

WX4400# clear authentication web ssid research temp*@thiscorp.com

See Also

- clear authentication admin on page 262
- clear authentication console on page 263
- clear authentication dot1x on page 264
- clear authentication mac on page 265
- clear authentication mac on page 265
- set authentication web on page 302
- display aaa on page 277

clear location policy

Removes a rule from the location policy on a WX switch.

Syntax — clear location policy rule-number

rule-number — Index number of a location policy rule to remove from the location policy.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To determine the index numbers of location policy rules, use the display location policy command. Removing all the ACEs from the location policy disables this function on the WX switch.

Examples — The following command removes location policy rule 4 from an WX switch’s location policy:

WX4400# clear location policy 4
success: clause 4 is removed.
clear mac-user

Removes a user profile from the local database on the WX for a user authenticated by a MAC address.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `clear mac-user mac-addr`

- **mac-addr** — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Deleting a MAC user’s profile from the database deletes the assignment of any attributes in the profile to the user.

**Examples** — The following command removes the user profile for a user at MAC address 01:02:03:04:05:06:

```
WX4400# clear mac-user 01:02:03:04:05:06
success: change accepted.
```

**See Also**

- `display aaa` on page 277
- `set mac-usergroup attr` on page 315
- `set mac-user attr` on page 309
clear mac-user attr

Removes an authorization attribute from the user profile in the local database on the WX switch, for a user who is authenticated by a MAC address.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `clear mac-user mac-addr attr attribute-name`

- `mac-addr` — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- `attribute-name` — Name of an attribute used to authorize the MAC user for a particular service or session characteristic. (For a list of authorization attributes, see Table 45 on page 310.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command removes an access control list (ACL) from the profile of a user at MAC address 01:02:03:04:05:06:

```
WX4400# clear mac-user 01:02:03:04:05:06 attr filter-id
success: change accepted.
```

**See Also**

- `display aaa` on page 277
- `set mac-user attr` on page 309

---

clear mac-user group

Removes a user group from the local database on the WX for a group of users authenticating with a MAC address.

(To remove a MAC user group profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `clear mac-user mac-addr group`

- `mac-addr` — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.

**Defaults** — None.
Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Removing a MAC user from a MAC user group removes the group name from the user’s profile, but does not delete the user group from the local WX database. To remove the group, use `clear mac-usergroup`.

Examples — The following command deletes the user profile for a user at MAC address 01:02:03:04:05:06 from its user group:

```
WX4400# clear mac-user 01:02:03:04:05:06 group
success: change accepted.
```

See Also

- `clear mac-usergroup` on page 270
- `display aaa` on page 277
- `set mac-user` on page 308

**clear mac-usergroup**

Removes a user group from the local database on the WX for a group of users authenticating with a MAC address.

(To delete a MAC user group in RADIUS, see the documentation for your RADIUS server.)

Syntax — `clear mac-usergroup group-name`

- `group-name` — Name of an existing MAC user group.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To remove a user from a MAC user group, use the `clear mac-user group` command.

Examples — The following command deletes the MAC user group `eastcoasters` from the local database:

```
WX4400# clear mac-usergroup eastcoasters
success: change accepted.
```
clear mac-usergroup attr

Removes an authorization attribute from a MAC user group in the local database on the WX, for a group of users who are authenticated by a MAC address. (To unconfigure an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — clear mac-usergroup group-name attr attribute-name

- `group-name` — Name of an existing MAC user group.
- `attribute-name` — Name of an attribute used to authorize the MAC users in the user group for a particular service or session characteristic. (For a list of authorization attributes, see Table 45 on page 310.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To remove the group itself, use the clear mac-usergroup command.

**Examples** — The following command removes the members of the MAC user group eastcoasters from a VLAN assignment by deleting the VLAN-Name attribute from the group:

```
WX4400# clear mac-usergroup eastcoasters attr vlan-name
success: change accepted.
```

**See Also**

- clear mac-usergroup on page 270
- display aaa on page 277
- set mac-usergroup attr on page 315
clear mobility-profile

Removes a Mobility Profile entirely.

**Syntax** — clear mobility-profile name

- **name** — Name of an existing Mobility Profile.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command removes the Mobility Profile for user Nin:

WX1200# clear mobility-profile Nin
success: change accepted.

**See Also**
- set mobility-profile on page 317
- set mobility-profile mode on page 319
- display mobility-profile on page 283

---

clear user

Removes a user profile from the local database on the WX, for a user with a password.

(To remove a user profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — clear user username

- **username** — Username of a user with a password.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Deleting the user profile from the database deletes the assignment of any profile attributes to the user.
Examples — The following command deletes the user profile for user Nin:

WX4400# clear user Nin
success: change accepted.

See Also
- display aaa on page 277
- set user on page 319

clear user attr

Removes an authorization attribute from the user profile in the local database on the WX for a user with a password.

(To remove an authorization attribute from a RADIUS user profile, see the documentation for your RADIUS server.)

Syntax — clear user username attr attribute-name
- username — Username of a user with a password.
- attribute-name — Name of an attribute used to authorize the user for a particular service or session characteristic. (For a list of authorization attributes, see Table 45 on page 310.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command removes the Session-Timeout attribute from Hosni’s user profile:

WX4400# clear user Hosni attr session-timeout
success: change accepted.

See Also
- display aaa on page 277
- set user attr on page 321
**clear user group**

Removes a user with a password from membership in a user group in the local database on the WX.

(To remove a user from a user group in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — clear user *username* group

- *username* — Username of a user with a password.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Removing the user from the group removes the group name from the user profile, but does not delete either the user or the user group from the local WX database. To remove the group, use `clear usergroup`.

**Examples** — The following command removes the user Nin from a user group:

```
WX4400# clear user Nin group
success: change accepted.
```

**See Also**

- *clear usergroup* on page 275
- *display aaa* on page 277
- *set user group* on page 323

**clear user lockout**

Restores access to a user who has been locked out of the system due to an expired password or exceeding the maximum number of failed login attempts.

**Syntax** — clear user *username* lockout

**Defaults** — None.

**Access** — Enabled.
clear usergroup

Removes a user group and its attributes from the local database on the WX, for users with passwords.

(To delete a user group in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `clear usergroup group-name`

- `group-name` — Name of an existing user group.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Removing a user group from the local WX database does not remove the user profiles of the group members from the database.

**Examples** — The following command deletes the cardiology user group from the local database:

```
WX4400# clear usergroup cardiology
success: change accepted.
```
See Also

- `clear usergroup attr` on page 276
- `display aaa` on page 277
- `set usergroup` on page 323

**clear usergroup attr**

Removes an authorization attribute from a user group in the local database on the WX.

(To remove an authorization attribute in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — clear usergroup group-name attr attribute-name

- `group-name` — Name of an existing user group.
- `attribute-name` — Name of an attribute used to authorize all the users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 45 on page 310.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command removes the members of the user group `cardiology` from a network access time restriction by deleting the Time-Of-Day attribute from the group:

```
WX4400# clear usergroup cardiology attr time-of-day
success: change accepted.
```

See Also

- `clear usergroup` on page 275
- `display aaa` on page 277
- `set usergroup` on page 323
**display aaa**

Displays all current AAA settings.

**Syntax** — `display aaa`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Web Portal section added, to indicate the state of the WebAAA feature in MSS Version 4.0.

**Examples** — To display all current AAA settings, type the following command:

WX4400# **display aaa**

Default Values
authport=1812 acctport=1813 timeout=5 acct-timeout=5
retrans=3 deadtime=0 key=(null) author-pass=(null)

Radius Servers

<table>
<thead>
<tr>
<th>Server</th>
<th>Addr</th>
<th>Ports</th>
<th>T/o</th>
<th>Tries</th>
<th>Dead</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>rs-3</td>
<td>198.162.1.1</td>
<td>1821</td>
<td>1813</td>
<td>5</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>rs-4</td>
<td>198.168.1.2</td>
<td>1821</td>
<td>1813</td>
<td>77</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>rs-5</td>
<td>198.162.1.3</td>
<td>1821</td>
<td>1813</td>
<td>42</td>
<td>23</td>
<td>0</td>
</tr>
</tbody>
</table>

Server groups
sg1: rs-3
sg2: rs-4
sg3: rs-5

Web Portal:
enabled

set authentication admin Jose sg3
set authentication console * none
set authentication mac ssid mycorp * local
set authentication dot1x ssid mycorp Geetha eap-tls
set authentication dot1x ssid mycorp * peap-mschapv2 sg1 sg2 sg3
set authentication dot1x ssid any ** peap-mschapv2 sg1 sg2 sg3
set accounting dot1x Nin ssid mycorp stop-only sg2
set accounting admin Natasha start-stop local

user Nin
Password = 082c6c64060b (encrypted)
Filter-Id = acl-999.in
Filter-Id = acl-999.out
user last-resort-guestssid
Vlan-Name = k2
user last-resort-any
Vlan-Name = foo
mac-user 01:02:03:04:05:06
usergroup eastcoasters
    session-timeout = 99

Table 43 describes the fields that can appear in display aaa output.

**Table 43** display aaa Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Values</td>
<td>RADIUS default values for all parameters.</td>
</tr>
<tr>
<td>authport</td>
<td>UDP port on the WX for transmission of RADIUS authorization and authentication messages. The default port is 1812.</td>
</tr>
<tr>
<td>acctport</td>
<td>UDP port on the WX for transmission of RADIUS accounting records. The default is port 1813.</td>
</tr>
<tr>
<td>timeout</td>
<td>Number of seconds the WX switch waits for a RADIUS server to respond before retransmitting. The default is 5 seconds.</td>
</tr>
<tr>
<td>acct-timeout</td>
<td>Number of seconds the WX waits for a RADIUS server to respond to an accounting request before retransmitting. The default is 5 seconds.</td>
</tr>
<tr>
<td>retrans</td>
<td>Number of times the WX switch retransmits a message before determining a RADIUS server unresponsive. The default is 3 times.</td>
</tr>
<tr>
<td>deadtime</td>
<td>Number of minutes the WX switch waits after determining a RADIUS server is unresponsive before trying to reconnect with this server. During the dead time, the RADIUS server is ignored by the WX. The default is 0 minutes.</td>
</tr>
<tr>
<td>key</td>
<td>Shared secret key, or password, used to authenticate to a RADIUS server. The default is no key.</td>
</tr>
<tr>
<td>author-pass</td>
<td>Password used for authorization to a RADIUS server for MAC authentication. The client MAC address is sent as the username and the author-pass string is sent as the password.</td>
</tr>
<tr>
<td>Radius Servers</td>
<td>Information about active RADIUS servers.</td>
</tr>
<tr>
<td>Server</td>
<td>Name of each RADIUS server currently active.</td>
</tr>
<tr>
<td>Addr</td>
<td>IP address of each RADIUS server currently active.</td>
</tr>
<tr>
<td>Ports</td>
<td>UDP ports that the WX switch uses for authentication messages and for accounting records.</td>
</tr>
</tbody>
</table>
display aaa

See Also

- set accounting {admin | console} on page 283
- set authentication admin on page 287
- set authentication console on page 289
- set authentication dot1x on page 291
- set authentication mac on page 295
- set authentication mac on page 295
- set authentication web on page 302

Table 43  display aaa Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T/o</td>
<td>Setting of timeouts on each RADIUS server currently active.</td>
</tr>
<tr>
<td>Tries</td>
<td>Number of retransmissions configured for each RADIUS server currently active.</td>
</tr>
<tr>
<td>Dead</td>
<td>Length of time until the server is considered responsive again.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of each RADIUS server currently active:</td>
</tr>
<tr>
<td></td>
<td>- UP (operating)</td>
</tr>
<tr>
<td></td>
<td>- DOWN (unavailable)</td>
</tr>
<tr>
<td>Server groups</td>
<td>Names of RADIUS server groups and member servers configured on the WX switch.</td>
</tr>
<tr>
<td>Web Portal</td>
<td>State of the WebAAA feature:</td>
</tr>
<tr>
<td></td>
<td>- enabled</td>
</tr>
<tr>
<td></td>
<td>- disabled</td>
</tr>
<tr>
<td>set commands</td>
<td>List of commands used to configure AAA on the WX switch.</td>
</tr>
<tr>
<td>user and user group profiles</td>
<td>List of user and user group profiles stored in the local database on the WX switch.</td>
</tr>
</tbody>
</table>
display accounting statistics

Displays the AAA accounting records for wireless users. The records are stored in the local database on the WX.

(To display RADIUS accounting records, see the documentation for your RADIUS server.)

Syntax — display accounting statistics

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0. Formatting of output enhanced for readability in Version 4.2

Examples — To display the locally stored accounting records, type the following command:

WX4400# display accounting statistics
Dec 14 00:39:48
Acct-Status-Type=STOP
Acct-Authentic=0
Acct-Multi-Session-Id=SESS-3-01f82f-520236-24bb1223
Acct-Session-Id=SESS-3-01f82f-520236-24bb1223
User-Name=vineet
AAA_ACCT_SVC_ATTR=2
Acct-Session-Time=551
Event-Timestamp=1134520788
Acct-Output-Octets=3204
Acct-Input-Octets=1691
Acct-Output-Packets=20
Acct-Input-Packets=19
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x

Dec 14 00:39:53
Acct-Status-Type=START
Acct-Authentic=0
User-Name=vineet
Acct-Multi-Session-Id=SESS-4-01f82f-520793-bd779517
Acct-Session-Id=SESS-4-01f82f-520793-bd779517
Event-Timestamp=1134520793
AAA_ACCT_SVC_ATTR=2
AAA_VLAN_NAME_ATTR=default
Calling-Station-Id=00-06-25-12-06-38
Nas-Port-Id=3/1
Called-Station-Id=00-0B-0E-00-CC-01
AAA_SSID_ATTR=vineet-dot1x

Table 44 describes the fields that can appear in **display accounting statistics** output.

| **Table 44** display accounting statistics Output |
|---|---|
| **Field** | **Description** |
| Date and time | Date and time of the accounting record. |
| Acct-Status-Type | Type of accounting record: |
| | • START |
| | • STOP |
| | • UPDATE |
| Acct-Authentic | Location where the user was authenticated (if authentication took place) for the session: |
| | • 1 — RADIUS server |
| | • 2 — Local WX database |
| User-Name | Username of a user with a password. |
| Acct-Multi-Session-Id | Unique accounting ID for multiple related sessions in a log file. |
| AAA_TTY_ATTR | For sessions conducted through a console or administrative Telnet connection, the Telnet terminal number. |
| Event-Timestamp | Time (in seconds since January 1, 1970) at which the event was triggered. (See RFC 2869 for more information.) |
| Acct-Session-Time | Number of seconds that the session has been online. |
| Acct-Output-Octets | Number of octets the WX has sent during the session. |
| Acct-Input-Octets | Number of octets the WX has received during the session. |
| Acct-Output-Packets | Number of packets the WX has sent during the session. |
| Acct-Input-Packets | Number of packets the WX has received during the session. |
| Vlan-Name | Name of the client VLAN. |
| Calling-Station-Id | MAC address of the supplicant (client). |
CHAPTER 8: AAA COMMANDS

Table 44  display accounting statistics Output (continued)

<table>
<thead>
<tr>
<th>Nas-Port-Id</th>
<th>Number of the port and radio on the MAP through which the session was conducted.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called-Station-Id</td>
<td>MAC address of the MAP through which the client reached the network.</td>
</tr>
</tbody>
</table>

See Also
- clear accounting on page 261
- display aaa on page 277
- set accounting {admin | console} on page 283

display location policy

Displays the list of location policy rules that make up the location policy on an WX switch.

Syntax — display location policy

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the list of location policy rules in the location policy on an WX switch:

WX4400 display location policy

<table>
<thead>
<tr>
<th>Id Clauses</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) deny if user eq *.theirfirm.com</td>
</tr>
<tr>
<td>2) permit vlan guest_1 if vlan neq *.wodefirm.com</td>
</tr>
<tr>
<td>3) permit vlan bld4.tac inacl tac_24.in if user eq *.ny.wodefirm.com</td>
</tr>
</tbody>
</table>

See Also
- clear location policy on page 267
- set location policy on page 304
**display mobility-profile**

Displays the named Mobility Profile. If you do not specify a Mobility Profile name, this command shows all Mobility Profile names and port lists on the WX.

**Syntax**

```plaintext
display mobility-profile [name]
```

- `name` — Name of an existing Mobility Profile.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays the Mobility Profile `magnolia`:

```plaintext
WX1200# display mobility-profile magnolia
Mobility Profiles
Name                Ports
========================
magnolia        AP 2
```

**See Also**

- `clear mobility-profile` on page 272
- `set mobility-profile` on page 317

**set accounting**

Sets up accounting services for specified wireless users with administrative access, and defines the accounting records and where they are sent.

**Syntax**

```plaintext
set accounting {admin | console} {user-glob} {start-stop | stop-only} method1 [method2] [method3] [method4]
```

- `admin` — Users with administrative access to the WX switch through Telnet or Web View.
- `console` — Users with administrative access to the WX switch through a console connection.
- `user-glob` — Single user or set of users with administrative access or network access.
CHAPTER 8: AAA COMMANDS

- Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

This option does not apply if mac is specified. For mac, specify a mac-addr-glob. (See “MAC Address Globs” on page 79.)

- `start-stop` — Sends accounting records at the start and end of a network session.
- `stop-only` — Sends accounting records only at the end of a network session.
- `method1, method2, method3, method4` — At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.

A method can be one of the following:

- `local` — Stores accounting records in the local database on the WX switch. When the local accounting storage space is full, MSS overwrites older records with new ones.
- `server-group-name` — Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

**Defaults** — Accounting is disabled for all users by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — For network users with start-stop accounting whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

**Examples** — The following command issues start-and-stop accounting records at the local WX database for administrator Natasha, when she accesses the switch using Telnet or Web Manager:

```
WX4400# set accounting admin Natasha start-stop local
success: change accepted.
```
set accounting \{dot1x | mac | web | last-resort\}

Sets up accounting services for specified wireless users with network access, and defines the accounting records and where they are sent.

**Syntax**

```
set accounting \{dot1x | mac | web | last-resort\} {ssid ssid-name | wired} {user-glob | mac-addr-glob} {start-stop | stop-only} method1 [method2] [method3] [method4]
```

- **dot1x** — Users with network access through the WX switch who are authenticated by 802.1X.
- **mac** — Users with network access through the WX switch who are authenticated by MAC authentication.
- **web** — Users with network access through the WX switch who are authenticated by WebAAA.
- **ssid ssid-name** — SSID name to which this accounting rule applies. To apply the rule to all SSIDs, type any.
- **wired** — Applies this accounting rule specifically to users who are authenticated on a wired authentication port.
- **user-glob** — Single user or set of users with administrative access or network access.
  Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character — either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

*This option does not apply if mac or last-resort is specified. For mac, specify a mac-addr-glob. (See “MAC Address Globs” on page 79.)*

- **mac-addr-glob** — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 79.)

This option applies only when mac is specified.

---

**See Also**

- `clear accounting` on page 261
- `display accounting statistics` on page 280
• **start-stop** — Sends accounting records at the start and end of a network session.

• **stop-only** — Sends accounting records only at the end of a network session.

• **method1, method2, method3, method4** — At least one of up to four methods that MSS uses to process accounting records. Specify one or more of the following methods in priority order. If the first method does not succeed, MSS tries the second method, and so on.

A method can be one of the following:

• **local** — Stores accounting records in the local database on the WX switch. When the local accounting storage space is full, MSS overwrites older records with new ones.

• **server-group-name** — Stores accounting records on one or more Remote Authentication Dial-In User Service (RADIUS) servers. You can also enter the names of existing RADIUS server groups as methods.

**Defaults** — Accounting is disabled for all users by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — For network users with start-stop accounting profiles whose records are sent to a RADIUS server, MSS sends interim updates to the RADIUS server when the user roams.

**Examples** — The following command issues stop-only records to the RADIUS server group *sg2* for network user Nin, who is authenticated by 802.1X:

```
WX4400# set accounting dot1x Nin stop-only sg2
success: change accepted.
```

**See Also**

• **clear accounting** on page 261

• **display accounting statistics** on page 280
set authentication admin

Configures authentication and defines where it is performed for specified users with administrative access through Telnet or Web Manager.

Syntax — set authentication admin
user-glob method1 [method2] [method3] [method4]

- **user-glob** — Single user or set of users with administrative access over the network through Telnet or Web Manager.
  Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

- **method1, method2, method3, method4** — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.
  A method can be one of the following:
  
  - **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
  
  - **server-group-name** — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

- **none** — For users with administrative access only, MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

**The authentication method none you can specify for administrative access is different from the falthru authentication type none, which applies only to network access. The authentication method none allows access to the WX switch by an administrator. The falthru authentication type none denies access to a network user. (See “set service-profile auth-falthru” on page 482.)**

For more information, see “Usage.”

**Defaults** — By default, authentication is deactivated for all admin users. The default authentication method in an admin authentication rule is **local**. MSS checks the local WX database for authentication.

**Access** — Enabled.
History — Introduced in MSS Version 3.0.

The syntax descriptions for the set authentication commands are separated for clarity. However, the options and behavior for the set authentication admin command are the same as in previous releases.

Usage — You can configure different authentication methods for different groups of users. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 78.)

If you specify multiple authentication methods in the set authentication console command, MSS applies them in the order that they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if local appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.

If a AAA rule specifies local as a secondary AAA method, to be used if the RADIUS servers are unavailable, and MSS authenticates a client with the local method, MSS starts again at the beginning of the method list when attempting to authorize the client. This can cause unexpected delays during client processing and can cause the client to time out before completing logon.

Examples — The following command configures administrator Jose, who connects via Telnet, for authentication on RADIUS server group sg3:

WX4400# set authentication admin Jose sg3
success: change accepted.

See Also
- clear authentication admin on page 262
- display aaa on page 277
- set authentication console on page 289
- set authentication dot1x on page 291
- set authentication mac on page 295
set authentication console

Configures authentication and defines where it is performed for specified users with administrative access through a console connection.

**Syntax** — `set authentication console user-glob method1 [method2] [method3] [method4]`

- `user-glob` — Single user or set of users with administrative access through the switch’s console.
  
  Specify a username, use the double-asterisk wildcard character (`**`) to specify all usernames, or use the single-asterisk wildcard character (`*`) to specify a set of usernames up to or following the first delimiter character—either an at sign (`@`) or a period (`.`). (For details, see “User Globs” on page 78.)

- `method1, method2, method3, method4` — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

  A method can be one of the following:

  - `local` — Uses the local database of usernames and user groups on the WX switch for authentication.
  - `server-group-name` — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.
  - `none` — For users with administrative access only, MSS performs no authentication, but prompts for a username and password and accepts any combination of entries, including blanks.

The authentication method `none` you can specify for administrative access is different from the falthru authentication type `none`, which applies only to network access. The authentication method `none` allows access to the WX switch by an administrator. The falthru authentication type `none` denies access to a network user. (See “set service-profile auth-falthru” on page 482.)
Defaults — By default, authentication is deactivated for all console users, and the default authentication method in a console authentication rule is **none**. MSS requires no username or password, by default. These users can press Enter at the prompts for administrative access.

It is recommended that you change the default setting unless the WX is in a secure physical location.

Access — Enabled.

History — Introduced in MSS Version 3.0.

The syntax description for the set authentication commands are separated for clarity. However, the options and behavior for the set authentication console command are the same as in previous releases.

Usage — You can configure different authentication methods for different groups of users. (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 78.)

If you specify multiple authentication methods in the set authentication console command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if **local** appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.

Examples — To set the console port so that it does not enforce username-password authentication for administrators, type the following command:

```
WX4400# set authentication console * none
success: change accepted.
```

See Also

- clear authentication console on page 263
- display aaa on page 277
set authentication dot1x

Configures authentication and defines how it is performed for specified wireless or wired authentication clients who use an IEEE 802.1X authentication protocol to access the network through the WX.

Syntax — set authentication dot1x {ssid ssid-name | wired} user-glob [bonded] protocol method1 [method2] [method3] [method4]

- ssid ssid-name — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type any.
- wired — Applies this authentication rule specifically to users connected to a wired authentication port.
- user-glob — A single user or a set of users with 802.1X network access.

Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character — either an at sign (@) or a period (.). (For details, see “User globs” on page 78.)

- bonded — Enables Bonded Auth™ (bonded authentication). When this feature is enabled, MSS authenticates the user only if the computer the user is on has already been authenticated.
- protocol — Protocol used for authentication. Specify one of the following:
  - eap-md5 — Extensible Authentication Protocol (EAP) with message-digest algorithm 5. For wired authentication clients:
    - Uses challenge-response to compare hashes
    - Provides no encryption or integrity checking for the connection
  - eap-tls — EAP with Transport Layer Security (TLS):
Provides mutual authentication, integrity-protected negotiation, and key exchange

Requires X.509 public key certificates on both sides of the connection

Provides encryption and integrity checking for the connection

Cannot be used with RADIUS server authentication (requires user information to be in the WX local database)

- **peap-mschapv2** — Protected EAP (PEAP) with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP-V2). For wireless clients:
  - Uses TLS for encryption and data integrity checking and server-side authentication.
  - Provides MS-CHAP-V2 mutual authentication.
  - Only the server side of the connection needs a certificate.
  - The wireless client authenticates using TLS to set up an encrypted session. Then MS-CHAP-V2 performs mutual authentication using the specified AAA method.

- **pass-through** — MSS sends all the EAP protocol processing to a RADIUS server.

> EAP-MD5 does not work with Microsoft wired authentication clients.

- **method1, method2, method3, method4** — At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

  A method can be one of the following:

  - **local** — Uses the local database of usernames and user groups on the WX switch for authentication.

  - **server-group-name** — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

    RADIUS servers cannot be used with the EAP-TLS protocol.
**set authentication dot1x**  

**Defaults** — By default, authentication is unconfigured for all clients with network access through MAP ports or wired authentication ports on the WX switch. Connection, authorization, and accounting are also disabled for these users.

Bonded authentication is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can configure different authentication methods for different groups of users by “globbing.” (For details, see “User Globs” on page 78.)

You can configure a rule either for wireless access to an SSID, or for wired access through a WX wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify any to match on all SSID names. If the rule is for wired access, specify wired instead of an SSID name.

You cannot configure client authentication that uses both EAP-TLS protocol and one or more RADIUS servers. EAP-TLS authentication is supported only on the local WX database.

If you specify multiple authentication methods in the **set authentication dot1x** command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if local appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local WX database and sends an authentication request to the server group.

If the user does not support 802.1X, MSS attempts to perform MAC authentication for the user. In this case, if the WX configuration contains a **set authentication mac** command that matches the SSID the user is attempting to access and the user MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.
If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the fallthru authentication type configured for the SSID, which can be last-resort, web-portal (for WebAAA), or none.

**Examples** — The following command configures EAP-TLS authentication in the local WX database for SSID mycorp and 802.1X client Geetha:

```
WX4400# set authentication dot1x ssid mycorp Geetha eap-tls local
success: change accepted.
```

The following command configures PEAP-MS-CHAP-V2 authentication at RADIUS server groups sg1 through sg3 for all 802.1X clients at example.com who want to access SSID examplecorp:

```
WX4400# set authentication dot1x ssid examplecorp *@example.com peap-mschapv2 sg1 sg2 sg3
success: change accepted.
```

**See Also**

- **clear authentication dot1x** on page 264
- **display aaa** on page 277
- **set authentication admin** on page 287
- **set authentication console** on page 289
- **set authentication mac** on page 295
- **set authentication mac** on page 295
- **set authentication web** on page 302
- **set service-profile auth-fallthru** on page 482
**set authentication mac**

Confirms authentication and defines where it is performed for specified non-802.1X users with network access through a media access control (MAC) address.

**Syntax** — `set authentication mac {ssid ssid-name | wired} mac-addr-glob method1 [method2] [method3] [method4]`

- **ssid ssid-name** — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type `any`.
- **wired** — Applies this authentication rule specifically to users connected to a wired authentication port.
- **mac-addr-glob** — A single user or set of users with access via a MAC address. Specify a MAC address, or use the wildcard (*) character to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 79.)
- **method1, method2, method3, method4** — At least one of up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- **local** — Uses the local database of usernames and user groups on the WX switch for authentication.
- **server-group-name** — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

For more information, see “Usage.”

**Defaults** — By default, authentication is deactivated for all MAC users, which means MAC address authentication fails by default. When using RADIUS for authentication, the default password for a MAC user is the MAC address of the user.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can configure different authentication methods for different groups of MAC addresses by “globbing.” (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 78.)
If you specify multiple authentication methods in the set authentication mac command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if local appears first, followed by a RADIUS server group, MSS ignores any failed searches in the local WX database and sends an authentication request to the RADIUS server group.

If the WX configuration contains a set authentication mac command that matches the SSID the user is attempting to access and the user MAC address, MSS uses the method specified by the command. Otherwise, MSS uses local MAC authentication by default.

If the username does not match an authentication rule for the SSID the user is attempting to access, MSS uses the fallthru authentication type configured for the SSID, which can be last-resort, web (for WebAAA), or none.

Examples — To use the local WX database to authenticate all users who access the mycorp2 SSID by their MAC address, type the following command:

WX4400# set authentication ssid mycorp2 mac ** local
success: change accepted.

See Also
- clear authentication mac on page 265
- display aaa on page 277
- set authentication admin on page 287
- set authentication console on page 289
- set authentication dot1x on page 291
- set authentication mac on page 295
- set authentication web on page 302
set authentication max-attempts

Specifies the maximum number of login attempts users can make before being locked out of the system.

Syntax — set authentication max-attempts number

Defaults — For Telnet or SSH sessions, a maximum of 4 failed login attempts are allowed by default. For console or network sessions, an unlimited number of failed login attempts are allowed by default.

- number — Number of allowable login attempts for a user. You can specify a number between 0 – 2147483647. Specifying 0 causes the number of allowable login attempts to reset to the default values.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — Use this command to specify the maximum number of failed login attempts allowed for a user. If the user is unable to log in within the specified number of attempts, he or she is locked out of the system, and the user’s access must be manually restored with the clear user lockout command.

Examples — To allow users a maximum of 3 attempts to log into the system, type the following command:

WX# set authentication max-attempts 3

See Also
- clear user lockout on page 274
- set authentication minimum-password-length on page 299
- set authentication password-restrict on page 300
set authentication max-attempts

Specifies the maximum number of login attempts users can make before being locked out of the system.

Syntax — `set authentication max-attempts number`

- **number** — Number of allowable login attempts for a user. You can specify a number between 0 – 2147483647. Specifying 0 causes the number of allowable login attempts to reset to the default values.

Defaults — For Telnet or SSH sessions, a maximum of 4 failed login attempts are allowed by default. For console or network sessions, an unlimited number of failed login attempts are allowed by default.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — Use this command to specify the maximum number of failed login attempts allowed for a user. If the user is unable to log in within the specified number of attempts, he or she is locked out of the system, and the user’s access must be manually restored with the `clear user lockout` command.

Examples — To allow users a maximum of 3 attempts to log into the system, type the following command:

```
WX# set authentication max-attempts 3
success: change accepted.
```

See Also
- `clear user lockout` on page 274
- `set authentication minimum-password-length` on page 299
- `set authentication password-restrict` on page 300
set authentication minimum-password-length

Specifies the minimum allowable length for user passwords.

Syntax — set authentication minimum-password-length length

- length — Minimum number of characters that can be in a user password. You can specify a minimum password length between 0 – 32 characters. Specifying 0 removes the restriction on password length.

Defaults — By default, there is no minimum length for user passwords.

Access — Enabled.

History — Introduced in MSS 6.0.

Usage — Use this command to specify the minimum length for user passwords. When this command is configured, you cannot configure a password shorter than the specified length.

When you enable this command, MSS evaluates the passwords configured on the WX and displays a list of users whose password does not meet the minimum length restriction.

Examples — To set the minimum length for user passwords at 7 characters, type the following command:

WX# set authentication minimum-password-length 7
Warning: The following users have passwords that are shorter than the minimum password length:

dan
admin
user2
goofball

success: change accepted.

See Also

- clear user lockout on page 274
- set authentication minimum-password-length on page 299
- set user on page 319
**set authentication password-restrict**

Activates password restrictions for network and administrative users.

**Syntax** — `set authentication password-restrict {enable | disable}`

- **enable** — Enables password restrictions on the WX.
- **disable** — Disables password restrictions on the WX.

**Defaults** — By default the password restrictions are disabled.

**Access** — Enabled.

**History** — Introduced in MSS 6.0.

**Usage** — When this command is enabled, the following password restrictions take effect:

Passwords must be a minimum of 10 characters in length, and a mix of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each (for example, *Tre%Pag32!*).

A user cannot reuse any of his or her 10 previous passwords (not applicable to network users).

When a user changes his or her password, at least 4 characters must be different from the previous password.

When you enable the password restrictions, MSS evaluates the passwords configured on the WX switch and displays a list of users whose password does not meet the restriction on length and character types.

**Examples** — To enable password restrictions on the WX switch, type the following command:

```
WX# set authentication password-restrict enable
warning: the following users have passwords that do not have at least 2 each of upper-case letters, lower-case letters, numbers and special characters -
dan
admin
user1
user2
goofball
dang
success: change accepted.
```
set authentication proxy

Configures a proxy authentication rule for a third-party AP’s wireless users.

Syntax — set authentication proxy ssid ssid-name user-glob radius-server-group

- **ssid** ssid-name — SSID name to which this authentication rule applies.
- **user-glob** — A single user or a set of users. Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs, MAC Address Globs, and VLAN Globs” on page 78.)
- **radius-server-group** — A group of RADIUS servers used for authentication.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0.

Usage — AAA for third-party AP users has additional configuration requirements. See the “Configuring AAA for Users of Third-Party APs” section in the “Configuring AAA for Network Users” chapter of the Wireless LAN Switch and Controller Configuration Guide.

Examples — The following command configures a proxy authentication rule that matches on all usernames associated with SSID mycorp. MSS uses RADIUS server group srvgrpl to proxy RADIUS requests and hence to authenticate and authorize the users.

WX4400# set authentication proxy ssid mycorp ** srvgrpl
CHAPTER 8: AAA COMMANDS

See Also

- clear authentication proxy on page 266
- set radius proxy client on page 633
- set radius proxy port on page 634

set authentication web

Configures an authentication rule to allow a user to log in to the network using a web page served by the WX. The rule can be activated if the user is not otherwise granted or denied access by 802.1X, or granted access by MAC authentication.

Syntax — set authentication web {ssid ssid-name | wired} user-glob method1 [method2] [method3] [method4]

- user-glob — A single user or a set of users.
  Specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

- ssid ssid-name — SSID name to which this authentication rule applies. To apply the rule to all SSIDs, type any.

- wired — Applies this authentication rule specifically to users connected to a wired authentication port.

- method1, method2, method3, method4 — At least one and up to four methods that MSS uses to handle authentication. Specify one or more of the following methods in priority order. MSS applies multiple methods in the order you enter them.

A method can be one of the following:

- local — Uses the local database of usernames and user groups on the WX switch for authentication.

- server-group-name — Uses the defined group of RADIUS servers for authentication. You can enter up to four names of existing RADIUS server groups as methods.

  RADIUS servers cannot be used with the EAP-TLS protocol.

For more information, see “Usage.”
Defaults — By default, authentication is unconfigured for all clients with network access through MAP ports or wired authentication ports on the WX switch. Connection, authorization, and accounting are also disabled for these users.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can configure different authentication methods for different groups of users by “globbing.” (For details, see “User Globs” on page 78.)

You can configure a rule either for wireless access to an SSID, or for wired access through a WX wired authentication port. If the rule is for wireless access to an SSID, specify the SSID name or specify any to match on all SSID names. If the rule is for wired access, specify wired instead of an SSID name.

If you specify multiple authentication methods in the set authentication web command, MSS applies them in the order in which they appear in the command, with these results:

If the first method responds with pass or fail, the evaluation is final.

If the first method does not respond, MSS tries the second method, and so on.

However, if local appears first, followed by a RADIUS server group, MSS overrides any failed searches in the local WX database and sends an authentication request to the server group.

MSS uses a WebAAA rule only under the following conditions:

The client is not denied access by 802.1X or does not support 802.1X.

The client MAC address does not match a MAC authentication rule.

The fallthru method is web. (For a wireless authentication rule, the fallthru method is specified by the set service-profile auth-fallthru command. For a wired authentication rule, the fallthru method is specified by the auth-fall-thru option of the set port type wired-auth command.)
Examples — The following command configures a WebAAA rule in the local WX database for SSID ourcorp and userglob rnd*:

WX4400# set authentication web ssid ourcorp rnd* local
success: change accepted.

See Also

- clear authentication proxy on page 266
- display aaa on page 277
- set authentication admin on page 287
- set authentication console on page 289
- set authentication dot1x on page 291
- set authentication mac on page 295

set location policy

Creates and enables a location policy on a WX. The location policy enables you to locally set or change authorization attributes for a user after the user is authorized by AAA, without making changes to the AAA server.

Syntax — set location policy deny if { ssid operator ssid-name | vlan operator vlan-glob | user operator user-glob | port port-list | ap ap-num } [ before rule-number | modify rule-number ]

Syntax — set location policy permit
{ vlan vlan-name | inacl inacl-name | outacl outacl-name } if { ssid operator ssid-name | vlan operator vlan-glob | user operator user-glob | port port-list | ap ap-num } [ before rule-number | modify rule-number ]

- deny — Denies access to the network to users with attributes that match the location policy rule.
- permit — Allows access to the network or to a specified VLAN, and/or assigns a particular security ACL to users with attributes matching match the location policy rule.

Action options — For a permit rule, MSS changes the attributes assigned to the user to the values specified by the following options:

- vlan vlan-name — Name of an existing VLAN to assign to users with attributes matching the location policy rule.
- **inacl** *inacl-name* — Name of an existing security ACL to apply to packets sent to the WX with attributes matching the location policy rule.
  Optionally, you can add the suffix `.in` to the name.

- **outacl** *outacl-name* — Name of an existing security ACL to apply to packets sent from the WX with attributes matching the location policy rule.
  Optionally, you can add the suffix `.out` to the name.

- **Condition options** — MSS takes the action specified by the rule if all conditions in the rule are met. You can specify one or more of the following conditions:

  - **ssid operator ssid-name** — SSID with which the user is associated. The *operator* must be `eq`, which applies the location policy rule to all users associated with the SSID. Asterisks (wildcards) are not supported in SSID names. You must specify the complete SSID name.

  - **vlan operator vlan-glob** — VLAN-Name attribute assigned by AAA and condition that determines if the location policy rule applies. Replace *operator* with one of the following operands:
    - `eq` — Applies the location policy rule to all users assigned VLAN names matching `vlan-glob`.
    - `neq` — Applies the location policy rule to all users assigned VLAN names not matching `vlan-glob`.

  For `vlan-glob`, specify a VLAN name, use the double-asterisk wildcard character (**) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “VLAN Globs” on page 80.)

  - **user operator user-glob** — Username and condition that determines if the location policy rule applies. Replace *operator* with one of the following operands:
    - `eq` — Applies the location policy rule to all usernames matching `user-glob`.
    - `neq` — Applies the location policy rule to all usernames *not* matching `user-glob`.
For user-glob, specify a username, use the double-asterisk wildcard character (**) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

- **before** rule-number — Inserts the new location policy rule in front of another rule in the location policy. Specify the number of the existing location policy rule. (To determine the number, use the display location policy command.)

- **modify** rule-number — Replaces the rule in the location policy with the new rule. Specify the number of the existing location policy rule. (To determine the number, use the display location policy command.)

- **port** port-list — List of physical port(s) that determines if the location policy rule applies.

**Defaults** — By default, users are permitted VLAN access and assigned security ACLs according to the VLAN-Name and Filter-Id attributes applied to the users during normal authentication and authorization.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. SSID option added in MSS Version 3.2.

**Usage** — Only a single location policy is allowed per WX switch. Once configured, the location policy becomes effective immediately. To disable location policy operation, use the clear location policy command.

Conditions within a rule are AND’ed. All conditions in the rule must match for MSS to take the specified action. If the location policy contains multiple rules, MSS compares the user information to the rules one at a time, in the order the rules appear in the WX configuration file, beginning with the rule at the top of the list. MSS continues comparing until a user matches all conditions in a rule or until there are no more rules.

The order of rules in the location policy is important to ensure users are properly granted or denied access. To position rules within the location policy, use **before** rule-number and **modify** rule-number in the set location policy command, and the clear location policy rule-number command.
When applying security ACLs:

Use `inACL inacl-name` to filter traffic that enters the WX from users via a
MAP access port or wired authentication port, or from the network via a
network port.

Use `outACL outacl-name` to filter traffic sent from the switch to users via a
MAP access port or wired authentication port, or from the network via a
network port.

You can optionally add the suffixes `.in` and `.out` to `inACL-name` and
`outACL-name` so that they match the names of security ACLs stored in the
local WX database.

**Examples** — The following command denies network access to all users
at *.*.theirm.com, causing them to fail authorization:

```
WX4400# set location policy deny if user eq *.*.theirm.com
```

The following command authorizes access to the `guest_1` VLAN for all
users who are not at *.*.wodefirm.com:

```
WX4400# set location policy permit vlan guest_1 if user neq *.*.wodefirm.com
```

The following command authorizes users at *.*.ny.ourfirm.com to access
the `bld4.tac` VLAN instead, and applies the security ACL `tac_24` to the
traffic they receive:

```
WX4400# set location policy permit vlan bld4.tac
outACL tac_24 if user eq *.*.ny.ourfirm.com
```

The following command authorizes access to users on VLANs with names
matching `bld4.*` and applies security ACLs `svcs_2` to the traffic they send
and `svcs_3` to the traffic they receive:

```
WX4400# set location policy permit inACL svcs_2 outACL svcs_3
if vlan eq bldg4.*
```

The following command authorizes users entering the network on WX
ports 1 and 2 to use the `floor2` VLAN, overriding any settings from AAA:

```
WX4400# set location policy permit vlan floor2 if port 1-2
```
The following command places all users who are authorized for SSID `tempvendor_a` into VLAN `kiosk_1`:

```
WX1200# set location policy permit vlan kiosk_1 iff ssid eq tempvendor_a
success: change accepted
```

**See Also**
- `clear location policy` on page 267
- `display location policy` on page 282

---

**set mac-user**

Configures a user profile in the local database on the WX for a user who can authenticate by a MAC address, and optionally adds the user to a MAC user group.

(To configure a MAC user profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `set mac-user mac-addr [group group-name]`

- `mac-addr` — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- `group-name` — Name of an existing MAC user group.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — MSS does not require MAC users to belong to user groups.

Users authenticated by MAC address are authenticated only for network access through the WX. MSS does not support passwords for MAC users.

**Examples** — The following command creates a user profile for a user at MAC address `01:02:03:04:05:06` and assigns the user to the `eastcoasters` user group:

```
WX4400# set mac-user 01:02:03:04:05:06 group eastcoasters
success: change accepted.
```
set mac-user attr

Assigns an authorization attribute in the local database on the WX to a user authenticating with a MAC address.

(To assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `set mac-user mac-addr attr attribute-name value`

- `mac-addr` — MAC address of the user, in hexadecimal numbers separated by colons (:). You can omit leading zeros.
- `attribute-name value` — Name and value of an attribute used to authorize a MAC user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to local users, see Table 45.

---

**See Also**

- `clear mac-user` on page 268
- `display aaa` on page 277
### Table 45  Authentication Attributes for Local Users

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Valid Value(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>encryption-type</td>
<td>Type of encryption required for access by the client. Clients who attempt to use an unauthorized encryption method are rejected.</td>
<td>One of the following numbers that identifies an encryption algorithm:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 1—AES_CCM (Advanced Encryption Standard using Counter with CBC-MAC)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 2—Reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 4—TKIP (Temporal Key Integrity Protocol)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 8—WEP_104 (the default) (Wired-Equivalent Privacy protocol using 104 bits of key strength)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 16—WEP_40 (Wired-Equivalent Privacy protocol using 40 bits of key strength)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 32—NONE (no encryption)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 64—Static WEP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In addition to these values, you can specify a sum of them for a combination of allowed encryption types. For example, to specify WEP_104 and WEP_40, use 24.</td>
</tr>
<tr>
<td>end-date</td>
<td>Date and time user access expires.</td>
<td>Date and time, in the following format: YY/MM/DD-HH:MM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can use <strong>end-date</strong> alone or with <strong>start-date</strong>. You also can use <strong>start-date, end-date</strong>, or both in conjunction with <strong>time-of-day</strong>.</td>
</tr>
</tbody>
</table>
**filter-id**

Inbound or outbound ACL to apply to the user.

If configured in the WX local database, this attribute can be an access control list (ACL) to filter outbound or inbound traffic. Use the following format:

- `filter-id inboundacl.in`
- `filter-id outboundacl.out`

If you are configuring the attribute on a RADIUS server, the value field of filter-id can specify up to two ACLs. Any of the following are valid:

- `filter-id = "Profile=acl1"`
- `filter-id = "OutboundACL=acl2"`
- `filter-id = "Profile=acl1 OutboundACL=acl2"`

(Each example goes on a single line on the server.) The format in which to specify the values depends on the RADIUS server.

Regardless of whether the attributes are defined locally or on a RADIUS server, the ACLs must already be configured on the WX.

**Table 45** Authentication Attributes for Local Users (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>idle-timeout</td>
<td>This option is not implemented in the current MSS version.</td>
</tr>
<tr>
<td>mobility-profile</td>
<td>Mobility Profile attribute for the user. (For more information, see set mobility-profile on page 317.)</td>
</tr>
<tr>
<td>name</td>
<td>Name of an existing Mobility Profile, up to 32 alphanumeric characters, with no tabs or spaces.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If the Mobility Profile feature is enabled, and a user is assigned a Mobility Profile name that does not exist on the WX, the user is denied access.</td>
</tr>
</tbody>
</table>
Table 45  Authentication Attributes for Local Users (continued)

| service-type | Type of access requested by the user. | One of the following numbers:  
2—Framed; for network user access  
6—Administrative; for administrative access to the WX, with authorization to access the enabled (configuration) mode. The user must enter the **enable** command to access the enabled mode.  
7—NAS-Prompt; for administrative access to the nonenabled mode only. In this mode, the **enable** command is not available and the user cannot log in to the enabled mode.  
For administrative sessions, the WX always sends 6 (Administrative).  
The RADIUS server can reply with one of the values listed above.  
If the service-type is not set on the RADIUS server, administrative users receive NAS-Prompt access, and network users receive Framed access. |

| session-timeout | Maximum number of seconds for the user's session. | Number between 0 and 4,294,967,296 seconds (approximately 136.2 years). |

| ssid | SSID accessible by the user after authentication. | Name of the SSID you want the user to use. The SSID must be configured in a service profile, and the service profile must be used by a radio profile assigned to MAP radios in the Mobility Domain. |

| start-date | Date and time at which the user becomes eligible to access the network.  
MSS does not authenticate the user unless the attempt to access the network occurs at or after the specified date and time, but before the end-date (if specified). | Date and time, in the following format:  
YY/MM/DD-HH:MM  
You can use **start-date** alone or with **end-date**. You also can use **start-date, end-date**, or both in conjunction with **time-of-day**. |
**Table 45  Authentication Attributes for Local Users (continued)**

<table>
<thead>
<tr>
<th>time-of-day (network access mode only)</th>
<th>Day(s) and time(s) during which the user is permitted to log into the network.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>After authorization, the user session can last until either the Time-Of-Day range or the Session-Timeout duration (if set) expires, whichever is shorter.</td>
</tr>
</tbody>
</table>

One of the following:

- **never**—Access is always denied.
- **any**—Access is always allowed.
- **al**—Access is always allowed.
- One or more ranges of values that consist of one of the following day designations (required), and a time range in **hhmm-hhmm** 4-digit 24-hour format (optional):
  - **mo**—Monday
  - **tu**—Tuesday
  - **we**—Wednesday
  - **th**—Thursday
  - **fr**—Friday
  - **sa**—Saturday
  - **su**—Sunday
  - **wk**—Any day between Monday and Friday

Separate values or a series of ranges (except time ranges) with commas (,) or a vertical bar (|). Do not use spaces.

The maximum number of characters is 253.

For example, to allow access only on Tuesdays and Thursdays between 10 a.m. and 4 p.m., specify the following:

```
  time-of-day tu1000-1600,th1000-1600
```

To allow access only on weekdays between 9 a.m and 5 p.m., and on Saturdays from 10 p.m. until 2 a.m., specify the following:

```
  time-of-day wk0900-1700,sa2200-0200
```

(Also see the examples for set user attr on page 321.)

You can use **time-of-day** in conjunction with **start-date**, **end-date**, or both.
Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter `set mac-user attr` with the new value. To delete an attribute, use `clear mac-user attr`.

<table>
<thead>
<tr>
<th>Table 45 Authentication Attributes for Local Users (continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>url</strong> (network access mode only)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>vlan-name</strong> (network access mode only)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>acct-interim-interval</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group the MAC user is in, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is sooner than the start-date configured for the MAC user group the user is in, the MAC user's network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group's start date.

Examples — The following command assigns input access control list (ACL) acl-03 to filter packets from a user at MAC address 01:02:03:04:05:06:

```
WX4400# set mac-user 01:02:03:04:05:06 attr filter-id acl-03.in
success: change accepted.
```

The following command restricts a user at MAC address 06:05:04:03:02:01 to network access between 7 p.m. on Mondays and Wednesdays and 7 a.m. on Tuesdays and Thursdays:

```
WX4400# set mac-user 06:05:04:03:02:01 attr time-of-day mo1900-1159,tu0000-0700,we1900-1159,th0000-0700
success: change accepted.
```

See Also

- `clear mac-user attr` on page 269
- `display aaa` on page 277

---

**set mac-usergroup attr**

Creates a user group in the local database on the WX for users authenticated by a MAC address, and assigns authorization attributes for the group.

(To configure a user group and assign authorization attributes through RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `set mac-usergroup group-name attr attribute-name value`

- **group-name** — Name of a MAC user group. Specify a name of up to 32 alphanumeric characters, with no spaces.
attribute-name value — Name and value of an attribute used to authorize all MAC users in the group for a particular service or session characteristic. (For a list of authorization attributes, see Table 45 on page 310.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter set mac-usergroup attr with the new value. To delete an attribute, use clear mac-usergroup attr.

You can assign attributes to individual MAC users and to MAC user groups. If attributes are configured for a MAC user and also for the group of the MAC user, the attributes assigned to the individual MAC user take precedence for that user. For example, if the start-date attribute configured for a MAC user is earlier than the start-date configured for the MAC user group, the MAC user network access can begin as soon as the user start-date. The MAC user does not need to wait for the MAC user group start date.

Examples — The following command creates the MAC user group eastcoasters and assigns the group members to VLAN orange:

WX4400# set mac-usergroup eastcoasters attr vlan-name orange
success: change accepted.

See Also

- clear mac-usergroup attr on page 271
- display aaa on page 277
**set mobility-profile**  
Creates a Mobility Profile and specifies the MAP access point and/or wired authentication ports on the WX switch through which any user assigned to the profile is allowed access.

**Syntax**

```
set mobility-profile name name
  {port {none | all | port-list}} | {ap {none | all | ap-num}}
```

- **name** — Name of the Mobility Profile. Specify up to 32 alphanumeric characters, with no spaces.
- **none** — Prevents any user to whom this profile is assigned from accessing any MAP access point or wired authentication port on the WX switch.
- **all** — Allows any user to whom this profile is assigned to access all MAP access ports and wired authentication port on the WX switch.
- **port-list** — List of MAP access ports or wired authentication ports through which any user assigned this profile is allowed access. The same port can be used in multiple Mobility Profile port lists.
- **ap-num** — List of Distributed MAP connections through which any user assigned this profile is allowed access. The same Distributed MAP can be used in multiple Mobility Profile port lists.

**Defaults** — No default Mobility Profile exists on the WX. If you do not assign Mobility Profile attributes, all users have access through all ports, unless denied access by other AAA servers or by access control lists (ACLs).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To assign a Mobility Profile to a user or group, specify it as an authorization attribute in one of the following commands:

```
set user attr mobility-profile name
set usergroup attr mobility-profile name
set mac-user attr mobility-profile name
set mac-usergroup attr mobility-profile name
```

To enable the use of the Mobility Profile feature on the WX switch, use the **set mobility-profile mode** command.
CAUTION: When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local WX database or RADIUS server when no Mobility Profile of that name exists on the WX.

To change the ports in a profile, use **set mobility-profile** again with the updated port list.

**Examples** — The following commands create the Mobility Profile *magnolia*, which restricts user access to port 2; enable the Mobility Profile feature on the WX switch; and assign the *magnolia* Mobility Profile to user *Jose*.

```
WX1200# set mobility-profile name magnolia port 2
success: change accepted.
WX1200# set mobility-profile mode enable
success: change accepted.
WX1200# set user Jose attr mobility-profile magnolia
success: change accepted.
```

The following command adds port 3 to the *magnolia* Mobility Profile (which is already assigned to port 2):

```
WX1200# set mobility-profile name magnolia port 3
success: change accepted.
```

**See Also**
- [clear mobility-profile](#) on page 272
- [display mobility-profile](#) on page 283
- [set mac-user attr](#) on page 309
- [set mac-usergroup attr](#) on page 315
- [set mobility-profile mode](#) on page 319
- [set user attr](#) on page 321
- [set usergroup](#) on page 323
**set mobility-profile mode**

Enables or disables the Mobility Profile feature on the WX switch.

**CAUTION:** When the Mobility Profile feature is enabled, a user is denied access if assigned a Mobility-Profile attribute in the local WX database or RADIUS server when no Mobility Profile of that name exists on the WX.

**Syntax** — `set mobility-profile mode {enable | disable}`

- **enable** — Enables the use of the Mobility Profile feature on the WX.
- **disable** — Specifies that all Mobility Profile attributes are ignored by the WX.

**Defaults** — The Mobility Profile feature is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To enable the use of the Mobility Profile feature, type the following command:

```
WX1200# set mobility-profile mode enable
success: change accepted.
```

**See Also**

- `clear mobility-profile` on page 272
- `display mobility-profile` on page 283
- `set mobility-profile` on page 317

---

**set user**

Configures a user profile in the local database on the WX for a user with a password.

(To configure a user profile in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `set user username password [encrypted] string`

- **username** — Username of a user with a password.
encrypted — Indicates that the password string you entered is already in its encrypted form. If you use this option, MSS does not encrypt the displayed form of the password string, and instead displays the string exactly as you entered it. If you omit this option, MSS does encrypt the displayed form of the string.

password string — Password of up to 32 alphanumeric characters, with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Although MSS allows you to configure a user password for the special “last-resort” guest user, the password has no effect. Last-resort users can never access a WX in administrative mode and never require a password.

Examples — The following command creates a user profile for user Nin in the local database, and assigns the password goody:

WX4400# set user Nin password goody
success: User Nin created

The following command assigns the password chey3nne to the admin user:

WX4400# set user admin password chey3nne
success: User admin created

The following command changes Nin’s password from goody to 29Jan04:

WX4400# set user Nin password 29Jan04

See Also

- clear user on page 272
- display aaa on page 277
**set user attr**

Configures an authorization attribute in the local database on the WX switch for a user with a password.

(To assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `set user username attr attribute-name value`

- `username` — Username of a user with a password.
- `attribute-name value` — Name and value of an attribute you are using to authorize the user for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 45 on page 310.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To change the value of an attribute, enter `set user attr` with the new value. To delete an attribute, use `clear user attr`.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is sooner than the start-date configured for the user group the user is in, the user’s network access can begin as soon as the user start-date. The user does not need to wait for the user group’s start date.

**Examples** — The following command assigns user Tamara to VLAN orange:

```
WX4400# set user Tamara attr vlan-name orange
success: change accepted.
```

The following command assigns Tamara to the Mobility Profile tulip.

```
WX4400# set user Tamara attr mobility-profile tulip
success: change accepted.
```
The following command limits the days and times when user Student1 can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

WX4400# set user Student1 attr time-of-day Wk1700-0200,Sa,Su
success: change accepted.

See Also
- clear user attr on page 273
- display aaa on page 277

---

**set user expire-password-in**

Specifies how long a user password is valid before it must be reset.

**Syntax**

```
set user username expire-password-in time
```

- **username** — Username of a user with a password.
- **time** — How long the specified user’s password is valid. The amount of time can be specified in days (for example, 30 or 30d), hours (720h), or a combination of days and hours (30d12h).

**Defaults** — By default, user passwords do not expire.

**Access** — Enabled.

**History** — Introduced in MSS 6.0.

**Usage** — Use this command to specify how long a specified user's password is valid. After this amount of time, the user's password expires, and a new password must be set.

**Examples** — The following command sets user Student1’s password to be valid for 30 days:

WX# set user Student1 expire-password-in 30
success: change accepted.

See Also
- clear user lockout on page 274
- set authentication minimum-password-length on page 299
- set authentication password-restrict on page 300
- set user on page 319
**set user group**

Adds a user to a user group. The user must have a password and a profile that exists in the local database on the WX.

(To configure a user in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `set user username group group-name`

- `username` — Username of a user with a password.
- `group-name` — Name of an existing user group for password users.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — MSS does not require users to belong to user groups.

To create a user group, use the command `set usergroup`.

**Examples** — The following command adds user Hosni to the `cardiology` user group:

```
WX4400# set user Hosni group cardiology
success: change accepted.
```

**See Also**

- `clear user group` on page 274
- `display aaa` on page 277

---

**set usergroup**

Creates a user group in the local database on the WX for users and assigns authorization attributes for the group.

(To create user groups and assign authorization attributes in RADIUS, see the documentation for your RADIUS server.)

**Syntax** — `set usergroup group-name attr attribute-name value`

- `group-name` — Name of a group for password users. Specify a name of up to 32 alphanumeric characters, with no spaces.
attribute-name value — Name and value of an attribute you are using to authorize all users in the group for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to users, see Table 45 on page 310.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To change the value of an attribute, enter set usergroup attr with the new value. To delete an attribute, use clear usergroup attr.

To add a user to a group, user the command set user group.

You can assign attributes to individual users and to user groups. If attributes are configured for a user and also for the group the user is in, the attributes assigned to the individual user take precedence for that user. For example, if the start-date attribute configured for a user is sooner than the start-date configured for the user group the user is in, the user’s network access can begin as soon as the user start-date. The user does not need to wait for the user group’s start date.

Examples — The following command adds the user group cardiology to the local database and assigns all the group members to VLAN crimson:

```
WX4400# set usergroup cardiology attr vlan-name crimson
success: change accepted.
```

See Also

- clear usergroup on page 275
- clear usergroup attr on page 276
- display aaa on page 277
Specifies how long the passwords for the users in user group are valid before they must be reset.

Syntax set usergroup group-name expire-password-in time

- **group-name** — Name of a group for password users.
- **time** — How long the passwords for the users in the specified group are valid. The amount of time can be specified in days (for example, 30 or 30d), hours (720h), or a combination of days and hours (30d12h).

**Defaults** — By default, user passwords do not expire.

**Access** — Enabled.

**History** — Introduced in MSS 6.0.

**Usage** — Use this command to specify how long the passwords for the users in a group are valid. After this amount of time, the passwords expire, and must be reset.

**Examples** — The following command sets the passwords for the users in user group cardiology to be valid for 30 days:

```
WX# set usergroup cardiology expire-password-in 30
success: change accepted.
```

**See Also**
- clear user lockout on page 274
- set authentication minimum-password-length on page 299
- set authentication password-restrict on page 300
- set user on page 319
set web-portal

Globally enables or disables WebAAA on a WX switch.

**Syntax** — `set web-portal {enable | disable}`

- **enable** — Enables WebAAA on the switch.
- **disable** — Disables WebAAA on the switch.

**Defaults** — Enabled.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Command name changed from `set web-aaa` to `set web-portal`, to match change to portal-based implementation in MSS Version 4.0.

**Usage** — This command disables or reenables support for WebAAA. However, WebAAA has additional configuration requirements. For information, see the “Configuring AAA for Network Users” chapter in the *Wireless LAN Switch and Controller Configuration Guide*.

**Examples** — To disable WebAAA, type the following command:

```
WX4400# set web-portal disable
success: change accepted.
```

**See Also**

- `clear authentication proxy` on page 266
- `set service-profile auth-fallthru` on page 482
- `set user` on page 319
Use Mobility Domain commands to configure and manage Mobility Domain groups.

A Mobility Domain is a system of WX switches and MAP access points working together to support a roaming user (client). One WX acts as a seed switch, which maintains and distributes a list of IP addresses of the domain members.

3Com recommends that you run the same MSS version on all the WX switches in a Mobility Domain.

### Commands by Usage

This chapter presents Mobility Domain commands alphabetically. Use Table 46 to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Domain</td>
<td>set mobility-domain mode seed domain-name</td>
<td>336</td>
</tr>
<tr>
<td></td>
<td>set mobility-domain member</td>
<td>332</td>
</tr>
<tr>
<td></td>
<td>set mobility-domain mode member seed-ip</td>
<td>334</td>
</tr>
<tr>
<td></td>
<td>set mobility-domain mode secondary-seed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>domain-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display mobility-domain</td>
<td>329</td>
</tr>
<tr>
<td></td>
<td>display mobility-domain status</td>
<td>331</td>
</tr>
<tr>
<td></td>
<td>display mobility-domain config</td>
<td>330</td>
</tr>
<tr>
<td></td>
<td>display mobility-domain status</td>
<td>331</td>
</tr>
<tr>
<td></td>
<td>clear mobility-domain member</td>
<td>328</td>
</tr>
<tr>
<td></td>
<td>clear mobility-domain</td>
<td>328</td>
</tr>
<tr>
<td></td>
<td>set domain security</td>
<td>337</td>
</tr>
</tbody>
</table>
**clear mobility-domain**

Clears all Mobility Domain configuration and information from a WX, regardless of whether the WX is a seed or a member of a Mobility Domain.

**Syntax** — `clear mobility-domain`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command has no effect if the WX is not configured as part of a Mobility Domain.

**Examples** — To clear a Mobility Domain from a WX within the domain, type the following command:

```plaintext
WX1200# clear mobility-domain
success: change accepted.
```

**See Also**

- `clear mobility-domain member` on page 328
- `set mobility-domain member` on page 332
- `set mobility-domain mode member seed-ip` on page 334
- `set mobility-domain mode seed domain-name` on page 336

---

**clear mobility-domain member**

On the seed WX, removes the identified member from the Mobility Domain.

**Syntax** — `clear mobility-domain member ip-addr`

- `ip-addr` — IP address of the Mobility Domain member, in dotted decimal notation.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
**Usage** — This command has no effect if the WX member is not configured as part of a Mobility Domain or the current WX is not the seed.

**Examples** — The following command clears a Mobility Domain member with the IP address 192.168.0.1:

```
WX1200# clear mobility-domain member 192.168.0.1
```

**See Also**
- `set mobility-domain member` on page 332

---

**display mobility-domain**

On the seed WX, displays the Mobility Domain status and members.

**Syntax** — `display mobility-domain`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 1.0.

**Examples** — To display Mobility Domain status, type the following command:

```
WX# display mobility-domain

Mobility Domain name: Pleasanton (security required)

<table>
<thead>
<tr>
<th>Member</th>
<th>State</th>
<th>Type(*):active</th>
<th>Model</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.8.107.1</td>
<td>STATE_UP</td>
<td>SEED*</td>
<td>WX-20</td>
<td>6.0.1.0</td>
</tr>
<tr>
<td>10.10.10.66</td>
<td>STATE_DOWN</td>
<td>MEMBER</td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
```

**Table 47 display mobility-domain Output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Domain name</td>
<td>Name of the Mobility Domain</td>
</tr>
<tr>
<td>Member</td>
<td>IP addresses of the seed WX and members in the Mobility Domain</td>
</tr>
<tr>
<td>State</td>
<td>State of the WX in the Mobility Domain:</td>
</tr>
<tr>
<td></td>
<td>- STATE_UP</td>
</tr>
<tr>
<td></td>
<td>- STATE_DOWN</td>
</tr>
</tbody>
</table>

Table 47 display mobility-domain Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Role of the WX in the Mobility Domain:</td>
</tr>
<tr>
<td></td>
<td>• MEMBER</td>
</tr>
<tr>
<td></td>
<td>• SEED</td>
</tr>
<tr>
<td></td>
<td>• SECONDARY-SEED</td>
</tr>
<tr>
<td>Model</td>
<td>Mode of the WX</td>
</tr>
<tr>
<td>Version</td>
<td>MSS version running on the WX</td>
</tr>
</tbody>
</table>

See Also

- clear mobility-domain on page 328
- set mobility-domain member on page 332
- set mobility-domain mode member seed-ip on page 334

display mobility-domain config

Displays the configuration of the Mobility Domain.

Syntax — display mobility-domain config

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the Mobility Domain configuration:

WX# display mobility-domain config
This switch is the seed for domain dang-modo.
10.8.107.1 is a member
10.10.10.66 is a member

See Also

- clear mobility-domain on page 328
- display mobility-domain status on page 331
- set mobility-domain member on page 332
**display mobility-domain status**

On the seed WX, displays the Mobility Domain status and members.

**Syntax** — `display mobility-domain status`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To display Mobility Domain status, type the following command:

```
WX4400# display mobility-domain status
```

<table>
<thead>
<tr>
<th>Mobility Domain name: Pleasanton</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>192.168.253.11</td>
</tr>
<tr>
<td>192.168.253.12</td>
</tr>
<tr>
<td>192.168.253.14</td>
</tr>
</tbody>
</table>

Table 48 describes the fields in the display.

**Table 48  display mobility-domain Output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Domain name</td>
<td>Name of the Mobility Domain</td>
</tr>
<tr>
<td>Member</td>
<td>IP addresses of the seed WX switch and members in the Mobility Domain</td>
</tr>
<tr>
<td>State</td>
<td>State of the WX switch in the Mobility Domain:</td>
</tr>
<tr>
<td></td>
<td>• STATE_UP</td>
</tr>
<tr>
<td></td>
<td>• STATE_DOWN</td>
</tr>
<tr>
<td>Status</td>
<td>Role of the WX switch in the Mobility Domain:</td>
</tr>
<tr>
<td></td>
<td>• MEMBER</td>
</tr>
<tr>
<td></td>
<td>• SEED</td>
</tr>
</tbody>
</table>

**See Also**

- `clear mobility-domain` on page 328
- `set mobility-domain member` on page 332
- `set mobility-domain mode member seed-ip` on page 334
set mobility-domain member

On the seed WX, adds a member to the list of Mobility Domain members. If the current WX is not configured as a seed, this command is rejected.

**Syntax** — `set mobility-domain member ip-addr Key hex-bytes`

- `ip-addr` — IP address of the Mobility Domain member in dotted decimal notation.
- `Key hex-bytes` — Fingerprint of the public key to use for WX-WX security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example:

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command must be entered from the seed WX.

**Examples** — The following commands add three WX switches with the IP addresses 192.168.1.8, 192.168.1.9, and 192.168.1.10 as members of a Mobility Domain whose seed is the current WX:

```
WX4400# set mobility-domain member 192.168.1.8
success: change accepted.
WX4400# set mobility-domain member 192.168.1.9
success: change accepted.
WX4400# set mobility-domain member 192.168.1.10
success: change accepted.
```

**See Also**

- `clear mobility-domain member` on page 328
- `display mobility-domain config` on page 330
- `set mobility-domain mode seed domain-name` on page 336
set mobility-domain mode member secondary seed-ip

Sets the IP address of the secondary seed WX on a nonseed WX.

Syntax — set mobility-domain mode member secondary seed-ip secondary-seed-ip-addr key hex-bytes

- `secondary-seed-ip-addr` — IP address of the secondary seed, in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 1.0.

Examples — The following command sets the current WX switch as a nonseed member of the Mobility Domain whose secondary seed has the IP address 192.168.1.8:

```
WX4400# set mobility-domain mode member seed-ip 192.168.1.8
mode is: member
seed IP is: 192.168.1.8
```

See Also

- `clear mobility-domain` on page 328
- `display mobility-domain config` on page 330
set mobility-domain mode member seed-ip

On a nonseed WX, sets the IP address of the seed WX. This command is used on a member WX to configure it as a member. If the WX is currently part of another Mobility Domain or using another seed, this command overwrites that configuration.

**Syntax** — set mobility-domain mode member seed-ip *ip-addr* key *hex-bytes*

- *ip-addr* — IP address of the Mobility Domain member, in dotted decimal notation.
- *key* *hex-bytes* — Fingerprint of the public key to use for WX-WX security. Specify the key as 16 hexadecimal bytes. Use a colon between each byte, as in the following example:

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 1.0. Option key hex-bytes added in Version 5.0.

**Examples** — The following command sets the current WX as a nonseed member of the Mobility Domain whose seed has the IP address 192.168.1.8:

WX# set mobility-domain mode member secondary seed-ip 192.168.1.8

**See Also**
- clear mobility-domain on page 328
- display mobility-domain config on page 330
**set mobility-domain mode secondary-seed domain-name**

Sets the current WX as a secondary-seed device for the Mobility Domain.

**Syntax** — `set mobility-domain mode secondary-seed domain-name`

- `mob-domain-name` — Name of the Mobility Domain. Specify between 1 and 32 characters with no spaces.
- `seed-ip` — The address of the seed device in the Mobility Domain.
- `primary-seed-ip-addr` — The address of the seed device in the Mobility Domain.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 6.0.

**Usage** — You can optionally specify a secondary seed in a Mobility Domain. The secondary seed provides redundancy for the primary seed switch in the Mobility Domain. If the primary seed becomes unavailable, the secondary seed assumes the role of the seed switch. This allows the Mobility Domain to continue functioning if the primary seed becomes unavailable.

When the primary seed switch fails, the remaining members form a Mobility Domain, with the secondary seed taking over as the primary seed switch.

If countermeasures had been in effect on the primary seed, they are stopped while the secondary seed gathers RF data from the member switches. Once the secondary seed has rebuilt the RF database, countermeasures can be restored.

VLAN tunnels (other than those between the member switches and the primary seed) continue to operate normally.

Roaming and session statistics continue to be gathered, providing that the primary seed is uninvolved with roaming.

When the primary seed is restored, it resumes its role as the primary seed switch in the Mobility Domain. The secondary seed returns to its role as a regular member of the Mobility Domain.
### set mobility-domain mode seed domain-name

Creates a Mobility Domain by setting the current WX as the seed device and naming the Mobility Domain.

#### Syntax

```
set mobility-domain mode seed domain-name mob-domain-name
```

- **mob-domain-name** — Name of the Mobility Domain. Specify between 1 and 32 characters with no spaces.

#### Defaults

None.

#### Access

Enabled.

#### History

- Introduced in MSS Version 3.0. Version 4.2 increased the maximum length of mob-domain-name to 32 characters.

#### Usage

Before you use this command, the current WX must have its IP address set with the `set system ip-address` command. After you enter this command, all Mobility Domain traffic is sent and received from the specified IP address.

You must explicitly configure only one WX switch per domain as the seed. All other WX switches in the domain receive their Mobility Domain information from the seed.

#### Examples

The following command creates a Mobility Domain named Pleasanton with the current WX as the seed:

```
WX4400# set mobility-domain mode seed domain-name Pleasanton
mode is: seed
domain name is: Pleasanton
```
set domain security

Sets mobility domain security to required (enabled) or none (disabled) on the wireless LAN switch. The command needs to be entered on each wireless LAN switch that will participate as a member of the secure mobility domain.

**Syntax** — *set domain security {required | none}*

**Defaults** — Mobility domain security is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS 5.0.

**Usage** — Domain keys for all switches must be properly configured before enabling domain security on the wireless LAN switch.

**Examples** — The following command enables mobility domain security on the wireless LAN switch:

```
WX4400# set domain security required
success: change accepted.
```
Use Network Domain commands to configure and manage Network Domain groups.

A Network Domain is a group of geographically dispersed Mobility Domains that share information over a WAN link. This shared information allows a user configured on a WX in one Mobility Domain to establish connectivity on a WX in another Mobility Domain in the same Network Domain. The WX forwards the user traffic by creating a VLAN tunnel to a WX in the remote Mobility Domain.

In a Network Domain, one or more WX switches serve as a seed switch. At least one of the Network Domain seeds maintains a connection with each of the member WX switches in the Network Domain. The Network Domain seeds share information about the VLANs configured on their members, so that all the Network Domain seeds have a common database of VLAN information.

<table>
<thead>
<tr>
<th>Network Domain Commands by Usage</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>This chapter presents Network Domain commands alphabetically. Use Table 49 to locate commands in this chapter based on their use.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Table 49</strong> Network Domain Commands by Usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td><strong>Command</strong></td>
<td></td>
</tr>
<tr>
<td>Network Domain</td>
<td>set network-domain mode seed domain-name on page 348</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set network-domain mode member seed-ip on page 346</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set network-domain peer on page 347</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear network-domain on page 340</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear network-domain mode on page 341</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 10: NETWORK DOMAIN COMMANDS

340

Table 49  Network Domain Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear network-domain</td>
<td>clear network-domain peer on page 342</td>
</tr>
<tr>
<td></td>
<td>clear network-domain seed-ip on page 343</td>
</tr>
<tr>
<td></td>
<td>display network-domain on page 344</td>
</tr>
</tbody>
</table>

clear network-domain

Clears all Network Domain configuration and information from a WX, regardless of whether the WX is a seed or a member of a Network Domain.

Syntax — clear network-domain

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Examples — This command has no effect if the WX is not configured as part of a Network Domain.

To clear a Network Domain from a WX within the domain, type the following command:

WX1200# clear network-domain

This will clear all network-domain configuration. Would you like to continue? (y/n) [n] y
success: change accepted.

See Also

- set network-domain mode member seed-ip on page 346
- set network-domain peer on page 347
- set network-domain mode seed domain-name on page 348
**clear network-domain mode**

Removes the Network Domain seed or member configuration from the WX.

**Syntax** — `clear network-domain mode {seed | member}`

- **seed** — Clears the Network Domain seed configuration from the WX switch.
- **member** — Clears the Network Domain member configuration from the WX switch.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 4.1.

**Usage** — This command has no effect if the WX is not configured as part of a Network Domain.

**Examples** — The following command clears the Network Domain member configuration from the WX:

```
WX1200# clear network-domain mode member
success: change accepted.
```

The following command clears the Network Domain seed configuration from the WX:

```
WX1200# clear network-domain mode seed
success: change accepted.
```

**See Also**

- `set network-domain mode member seed-ip` on page 346
- `set network-domain mode seed domain-name` on page 348
clear network-domain peer

Removes the configuration of a Network Domain peer from a WX configured as a Network Domain seed.

**Syntax** — `clear network-domain peer {ip-addr | all}`

- `ip-addr` — IP address of the Network Domain peer in dotted decimal notation.
- `all` — Clears the Network Domain peer configuration for all peers from the WX switch.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 4.1.

**Usage** — This command has no effect if the WX is not configured as a Network Domain seed.

**Examples** — The following command clears the Network Domain peer configuration for peer 192.168.9.254 from the WX:

```
WX1200# clear network-domain peer 192.168.9.254
success: change accepted.
```

The following command clears the Network Domain peer configuration for all peers from the WX:

```
WX1200# clear network-domain peer all
success: change accepted.
```

**See Also**

- `set network-domain peer` on page 347
clear network-domain seed-ip

Removes the specified Network Domain seed from the WX configuration. When you enter this command, the Network Domain TCP connections between the WX switch and the specified Network Domain seed are closed.

Syntax — clear network-domain seed-ip ip-addr

- ip-addr — IP address of the Network Domain seed in dotted decimal notation.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — This command has no effect if the WX is not configured as part of a Network Domain, or if the WX is not configured as a member of a Network Domain that uses the specified Network Domain seed.

The following command removes the Network Domain seed with IP address 192.168.9.254 from the WX configuration:

WX1200# clear network-domain seed-ip 192.168.9.254
success: change accepted.

See Also

- set network-domain mode member seed-ip on page 346
display network-domain

Displays the status of Network Domain seeds and members.

**Syntax** — `display network-domain`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 4.1.

**Examples** — To display Network Domain status, type the following command. The output of the command differs based on whether the WX switch is a member of a Network Domain or a Network Domain seed.

On a WX that is a Network Domain member, the following output is displayed:

```
WX1200# display network-domain
Member Network Domain name: California
Member State Mode
--------------     -------
10.8.107.1        UP SEED
```

On a WX switch that is a Network Domain seed, information is displayed about the Network Domains of which the WX switch is a member, as well as Network Domain seeds with which the WX switch has a peer relationship. For example:

```
WX1200# display network-domain
Network Domain name: California
Peer State
-------------     -------
10.8.107.1 UP
Member State Mode
-------------- -------------  -----
10.1.0.0 DOWN SEED
Member Network Domain name:
Member State Mode
-------------- -------------  -----
10.8.107.1 UP MEMBER
10.1.0.0 DOWN SEED
```
Table 50 describes the fields in the display.

**Table 50  Radio-Specific Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Output if WX is the Network Domain Seed</strong></td>
<td></td>
</tr>
<tr>
<td>Network Domain name</td>
<td>Name of the Network Domain for which the WX is a seed.</td>
</tr>
<tr>
<td>Peer</td>
<td>IP addresses of the other seeds in the Network Domain.</td>
</tr>
<tr>
<td>State</td>
<td>State of the connection between the WX and the peer Network Domain seeds: UP, DOWN</td>
</tr>
<tr>
<td>Member</td>
<td>IP addresses of the seed WX and members in the Network Domain.</td>
</tr>
<tr>
<td>State</td>
<td>State of the WX in the Network Domain: UP, DOWN</td>
</tr>
<tr>
<td>Mode</td>
<td>Role of the WX in the Network Domain: UP, DOWN</td>
</tr>
<tr>
<td>Mobility-Domain</td>
<td>Name of the Mobility Domain of which the WX is a member.</td>
</tr>
<tr>
<td><strong>Output if WX is a Network Domain Member</strong></td>
<td></td>
</tr>
<tr>
<td>Member Network Domain name</td>
<td>Name of the Network Domain of which the WX is a member.</td>
</tr>
<tr>
<td>Member</td>
<td>IP addresses of the seed WX and members in the Network Domain.</td>
</tr>
<tr>
<td>State</td>
<td>State of the WX in the Network Domain. UP, DOWN</td>
</tr>
<tr>
<td>Mode</td>
<td>Role of the WX in the Network Domain: MEMBER, SEED</td>
</tr>
<tr>
<td>Mobility-Domain</td>
<td>Name of the Mobility Domain of which the WX is a member.</td>
</tr>
</tbody>
</table>

**See Also**
- `clear network-domain` on page 340
- `set network-domain mode member seed-ip` on page 346
- `set network-domain mode seed domain-name` on page 348
- `set network-domain peer` on page 347
Sets the IP address of a Network Domain seed. This command is used for configuring a WX as a member of a Network Domain. You can specify multiple Network Domain seeds and configure one as the primary seed.

Syntax — `set network-domain mode member seed-ip ip-addr [affinity num]`

- `ip-addr` — IP address of the Network Domain seed, in dotted decimal notation.
- `num` — Preference for using the specified Network Domain seed. You can specify a value from 1 through 10. A higher number indicates a greater preference.

Defaults — The default affinity for a Network Domain seed is 5.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — You can specify multiple Network Domain seeds on the WX. When the WX needs to connect to a Network Domain seed, it first attempts to connect to the seed with the highest affinity. If that seed is unavailable, the WX attempts to connect to the seed with the next-highest affinity. After a connection is made to a non-highest-affinity seed, the WX switch then periodically attempts to connect to the highest-affinity seed.

Examples — The following command sets the WX switch as a member of the Network Domain whose seed has the IP address 192.168.1.8:

```
WX1200# set network-domain mode member seed-ip 192.168.1.8
success: change accepted.
```

The following command sets the WX as a member of a Network Domain whose seed has the IP address 192.168.9.254 and sets the affinity for that seed to 7. If the WX specifies other Network Domain seeds, and they are configured with the default affinity of 5, then 192.168.9.254 becomes the primary Network Domain seed for this WX.

```
WX1200# set network-domain mode member seed-ip 192.168.9.254 affinity 7
success: change accepted.
```
**set network-domain peer**

On a Network Domain seed, configures one or more WX as redundant Network Domain seeds. The seeds in a Network Domain share information about the VLANs configured on the member devices, so that all the Network Domain seeds have the same database of VLAN information.

**Syntax** — `set network-domain peer ip-addr`

- `ip-addr` — IP address of the Network Domain seed to specify as a peer, in dotted decimal notation.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 4.1.

**Usage** — This command must be entered on a WX configured as a Network Domain seed.

**Examples** — The following command sets the WX switch with IP address 192.168.9.254 as a peer of this Network Domain seed:

```
WX1200# set network-domain peer 192.168.9.254
success: change accepted.
```

**See Also**

- `clear network-domain` on page 340
- `display network-domain` on page 344
set network-domain mode seed domain-name

Creates a Network Domain by setting the current WX as a seed device and naming the Network Domain.

Syntax — set network-domain mode seed domain-name

net-domain-name

- net-domain-name — Name of the Network Domain. Specify between 1 and 16 characters with no spaces.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.1.

Usage — Before you use this command, the current WX must have its IP address set with the set system ip-address command. After you enter this command, Network Domain traffic is sent and received from the specified IP address.

You can configure multiple WX switches as Network Domain seeds. If you do this, you must identify them as peers by using the set network domain peer command.

Examples — The following command creates a Network Domain named California with the current WX as a seed:

WX1200# set network-domain mode seed domain-name California
success: change accepted.

The seed switch in a Network Domain must also be configured as a member of the Network Domain, with the specified seed IP address pointing to the seed itself.

set network-domain mode member seed-ip ip-addr [affinity num]

For example, the following command sets the current WX switch as a member of a Network Domain where the WX switch with IP address 192.168.9.254 is a seed:

WX1200# set network-domain mode member seed-ip 192.168.9.254
success: change accepted.

See Also

- clear network-domain on page 340
- display network-domain on page 344
11 MANAGED ACCESS POINT COMMANDS

Use MAP access point commands to configure and manage MAP access points. Be sure to do the following before using the commands:

- Define the country-specific IEEE 802.11 regulations on the WX switch. (See set system countrycode on page 109.)
- Install the MAP access point and connect it to a port on the WX switch.
- Configure a MAP as a directly connected MAP or a Distributed MAP. (See set port type ap on page 145 and set ap on page 135.)

CAUTION: Changing the system country code after MAP configuration disables MAP access points and deletes their configuration. If you change the country code on a WX, you must reconfigure all MAP access points.

MAP Access Point Commands by Usage

This chapter presents MAP access point commands alphabetically. Use the following table to locate commands in this chapter based on their use.

Table 51  Map Access Point Commands by Usage

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Configuration of Distributed MAPs</td>
<td>set ap auto on page 410</td>
</tr>
<tr>
<td></td>
<td>set ap auto mode on page 414</td>
</tr>
<tr>
<td></td>
<td>set ap auto radiotype on page 413</td>
</tr>
<tr>
<td></td>
<td>set ap auto persistent on page 412</td>
</tr>
<tr>
<td></td>
<td>set ap bias on page 415</td>
</tr>
<tr>
<td></td>
<td>set ap blink on page 416</td>
</tr>
<tr>
<td></td>
<td>set ap group on page 427</td>
</tr>
<tr>
<td></td>
<td>set ap radio auto-tune max-power on page 432</td>
</tr>
</tbody>
</table>
Table 51  Map Access Point Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>set ap radio auto-tune max-retransmissions</strong></td>
<td>on page 433</td>
</tr>
<tr>
<td><strong>set ap radio link-calibration</strong></td>
<td>on page 436</td>
</tr>
<tr>
<td><strong>set ap radio mode</strong></td>
<td>on page 439</td>
</tr>
<tr>
<td><strong>set ap radio radio-profile</strong></td>
<td>on page 440</td>
</tr>
<tr>
<td><strong>set ap auto radiotype</strong></td>
<td>on page 413</td>
</tr>
<tr>
<td><strong>set ap upgrade-firmware</strong></td>
<td>on page 444</td>
</tr>
<tr>
<td><strong>External Antennas</strong></td>
<td><strong>set ap radio antennatype</strong></td>
</tr>
<tr>
<td></td>
<td>on page 431</td>
</tr>
<tr>
<td><strong>set ap radio antenna-location</strong></td>
<td>on page 430</td>
</tr>
<tr>
<td><strong>MAP-WX Security</strong></td>
<td><strong>set ap fingerprint</strong></td>
</tr>
<tr>
<td></td>
<td>on page 424</td>
</tr>
<tr>
<td><strong>set ap security</strong></td>
<td>on page 443</td>
</tr>
<tr>
<td><strong>Static IP Address Assignment for Distributed MAPs</strong></td>
<td><strong>set ap boot-configuration ip</strong></td>
</tr>
<tr>
<td></td>
<td>on page 417</td>
</tr>
<tr>
<td></td>
<td><strong>set ap boot-configuration switch</strong></td>
</tr>
<tr>
<td></td>
<td>on page 422</td>
</tr>
<tr>
<td></td>
<td><strong>set ap boot-configuration vlan</strong></td>
</tr>
<tr>
<td></td>
<td>on page 423</td>
</tr>
<tr>
<td></td>
<td><strong>clear ap boot-configuration</strong></td>
</tr>
<tr>
<td></td>
<td>on page 358</td>
</tr>
<tr>
<td></td>
<td><strong>display ap boot-configuration</strong></td>
</tr>
<tr>
<td></td>
<td>on page 390</td>
</tr>
<tr>
<td></td>
<td><strong>set ap upgrade-firmware</strong></td>
</tr>
<tr>
<td></td>
<td>on page 444</td>
</tr>
<tr>
<td><strong>Radio Profile Assignment</strong></td>
<td><strong>set ap radio radio-profile</strong></td>
</tr>
<tr>
<td></td>
<td>on page 440</td>
</tr>
<tr>
<td></td>
<td><strong>set radio-profile mode</strong></td>
</tr>
<tr>
<td></td>
<td>on page 464</td>
</tr>
<tr>
<td></td>
<td><strong>clear radio-profile</strong></td>
</tr>
<tr>
<td></td>
<td>on page 360</td>
</tr>
<tr>
<td></td>
<td><strong>set radio-profile service-profile</strong></td>
</tr>
<tr>
<td></td>
<td>on page 472</td>
</tr>
<tr>
<td></td>
<td><strong>display radio-profile</strong></td>
</tr>
<tr>
<td></td>
<td>on page 398</td>
</tr>
<tr>
<td><strong>SSID Assignment</strong></td>
<td><strong>set service-profile ssid-name</strong></td>
</tr>
<tr>
<td></td>
<td>on page 513</td>
</tr>
<tr>
<td></td>
<td><strong>set service-profile ssid-type</strong></td>
</tr>
<tr>
<td></td>
<td>on page 514</td>
</tr>
<tr>
<td></td>
<td><strong>set service-profile beacon</strong></td>
</tr>
<tr>
<td></td>
<td>on page 484</td>
</tr>
<tr>
<td><strong>Radio Properties</strong></td>
<td><strong>set radio-profile active-scan</strong></td>
</tr>
<tr>
<td></td>
<td>on page 448</td>
</tr>
<tr>
<td></td>
<td><strong>set radio-profile beacon-interval</strong></td>
</tr>
<tr>
<td></td>
<td>on page 457</td>
</tr>
<tr>
<td></td>
<td><strong>set radio-profile countermeasures</strong></td>
</tr>
<tr>
<td></td>
<td>on page 458</td>
</tr>
<tr>
<td></td>
<td><strong>set radio-profile dtim-interval</strong></td>
</tr>
<tr>
<td></td>
<td>on page 460</td>
</tr>
<tr>
<td></td>
<td><strong>set radio-profile frag-threshold</strong></td>
</tr>
<tr>
<td></td>
<td>on page 461</td>
</tr>
<tr>
<td></td>
<td><strong>set radio-profile max-rx-lifetime</strong></td>
</tr>
<tr>
<td></td>
<td>on page 462</td>
</tr>
</tbody>
</table>
Table 51  Map Access Point Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>set radio-profile max-tx-lifetime</td>
<td>463</td>
</tr>
<tr>
<td></td>
<td>set radio-profile preamble-length</td>
<td>467</td>
</tr>
<tr>
<td></td>
<td>set radio-profile rts-threshold</td>
<td>471</td>
</tr>
<tr>
<td>Authentication and Encryption</td>
<td>set service-profile attr</td>
<td>479</td>
</tr>
<tr>
<td></td>
<td>set service-profile auth-dot1x</td>
<td>481</td>
</tr>
<tr>
<td></td>
<td>set service-profile auth-fallthru</td>
<td>482</td>
</tr>
<tr>
<td></td>
<td>set service-profile web-portal-form</td>
<td>521</td>
</tr>
<tr>
<td></td>
<td>set service-profile web-portal-acl</td>
<td>520</td>
</tr>
<tr>
<td></td>
<td>set service-profile auth-psk</td>
<td>483</td>
</tr>
<tr>
<td></td>
<td>set service-profile wpa-ie</td>
<td>529</td>
</tr>
<tr>
<td></td>
<td>set service-profile rsn-ie</td>
<td>503</td>
</tr>
<tr>
<td></td>
<td>set service-profile cipher-ccmp</td>
<td>488</td>
</tr>
<tr>
<td></td>
<td>set service-profile cipher-tkip</td>
<td>489</td>
</tr>
<tr>
<td></td>
<td>set service-profile cipher-wep104</td>
<td>490</td>
</tr>
<tr>
<td></td>
<td>set service-profile cipher-wep40</td>
<td>491</td>
</tr>
<tr>
<td></td>
<td>set service-profile psk-phrase</td>
<td>501</td>
</tr>
<tr>
<td></td>
<td>set service-profile psk-raw</td>
<td>502</td>
</tr>
<tr>
<td></td>
<td>set service-profile tkip-mc-time</td>
<td>514</td>
</tr>
<tr>
<td></td>
<td>set service-profile wep active-multicast-</td>
<td>526</td>
</tr>
<tr>
<td></td>
<td>index</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set service-profile wep active-unicast-</td>
<td>527</td>
</tr>
<tr>
<td></td>
<td>index</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set service-profile wep key-index</td>
<td>528</td>
</tr>
<tr>
<td></td>
<td>set service-profile keep-initial-vlan</td>
<td>495</td>
</tr>
<tr>
<td></td>
<td>set service-profile transmit-rates</td>
<td>516</td>
</tr>
<tr>
<td></td>
<td>set service-profile long-retry-count</td>
<td>497</td>
</tr>
<tr>
<td></td>
<td>set service-profile short-retry-count</td>
<td>504</td>
</tr>
<tr>
<td></td>
<td>set service-profile shared-key-auth</td>
<td>504</td>
</tr>
<tr>
<td></td>
<td>display service-profile</td>
<td>401</td>
</tr>
<tr>
<td></td>
<td>clear service-profile</td>
<td>361</td>
</tr>
</tbody>
</table>
Table 51  Map Access Point Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>QoS and VoIP</strong></td>
<td>set radio-profile qos-mode on page 468</td>
</tr>
<tr>
<td></td>
<td>set radio-profile wmm-powersave on page 478</td>
</tr>
<tr>
<td></td>
<td>set service-profile cac-mode on page 486</td>
</tr>
<tr>
<td></td>
<td>set service-profile cac-session on page 487</td>
</tr>
<tr>
<td></td>
<td>set service-profile static-cos on page 515</td>
</tr>
<tr>
<td></td>
<td>set service-profile cos on page 492</td>
</tr>
<tr>
<td></td>
<td>set service-profile use-client-dscp on page 518</td>
</tr>
<tr>
<td><strong>DHCP Restrict</strong></td>
<td>set service-profile dhcp-restrict on page 493</td>
</tr>
<tr>
<td><strong>Broadcast Control</strong></td>
<td>set service-profile no-broadcast on page 499</td>
</tr>
<tr>
<td><strong>Proxy ARP</strong></td>
<td>set service-profile proxy-arp on page 500</td>
</tr>
<tr>
<td><strong>Keepalives and Session Timers</strong></td>
<td>set service-profile idle-client-probing on page 494</td>
</tr>
<tr>
<td></td>
<td>set service-profile user-idle-timeout on page 519</td>
</tr>
<tr>
<td></td>
<td>set service-profile web-portal-session-timeout on page 525</td>
</tr>
<tr>
<td><strong>Sygate On-Demand (SODA)</strong></td>
<td>set service-profile soda mode on page 510</td>
</tr>
<tr>
<td></td>
<td>set service-profile soda agent-directory on page 505</td>
</tr>
<tr>
<td></td>
<td>set service-profile soda enforce-checks on page 506</td>
</tr>
<tr>
<td></td>
<td>set service-profile soda failure-page on page 507</td>
</tr>
<tr>
<td></td>
<td>set service-profile soda remediation-ad on page 511</td>
</tr>
<tr>
<td></td>
<td>set service-profile soda success-page on page 512</td>
</tr>
<tr>
<td></td>
<td>set service-profile soda logout-page on page 508</td>
</tr>
<tr>
<td><strong>Radio Transmit Rates</strong></td>
<td>set service-profile transmit-rates on page 516</td>
</tr>
<tr>
<td></td>
<td>set radio-profile rate-enforcement on page 469</td>
</tr>
<tr>
<td><strong>Transmit Retries</strong></td>
<td>set service-profile long-retry-count on page 497</td>
</tr>
<tr>
<td></td>
<td>set service-profile short-retry-count on page 504</td>
</tr>
<tr>
<td><strong>RF Auto-Tuning</strong></td>
<td>set radio-profile auto-tune 11a-channel-range on page 449</td>
</tr>
<tr>
<td></td>
<td>set radio-profile auto-tune channel-holddown on page 451</td>
</tr>
<tr>
<td></td>
<td>set radio-profile auto-tune channel-interval on page 452</td>
</tr>
</tbody>
</table>
Table 51  Map Access Point Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>set radio-profile auto-tune channel-lockdown on page 453</td>
</tr>
<tr>
<td></td>
<td>set radio-profile auto-tune power-config on page 454</td>
</tr>
<tr>
<td></td>
<td>set radio-profile auto-tune power-interval on page 455</td>
</tr>
<tr>
<td></td>
<td>set radio-profile auto-tune power-lockdown on page 456</td>
</tr>
<tr>
<td></td>
<td>set ap radio auto-tune max-power on page 432</td>
</tr>
<tr>
<td></td>
<td>display auto-tune neighbors on page 388</td>
</tr>
<tr>
<td></td>
<td>display auto-tune attributes on page 386</td>
</tr>
<tr>
<td>AeroScout Tag Support</td>
<td>set radio-profile rfid-mode on page 469</td>
</tr>
<tr>
<td>Radio State</td>
<td>set ap radio mode on page 439</td>
</tr>
<tr>
<td>Dual Homing</td>
<td>set ap bias on page 415</td>
</tr>
<tr>
<td>RF Load Balancing</td>
<td>set ap radio load balancing on page 437</td>
</tr>
<tr>
<td></td>
<td>clear ap radio load-balancing group on page 359</td>
</tr>
<tr>
<td></td>
<td>set band-preference on page 445</td>
</tr>
<tr>
<td></td>
<td>set load-balancing mode on page 446</td>
</tr>
<tr>
<td></td>
<td>set load-balancing strictness on page 447</td>
</tr>
<tr>
<td></td>
<td>set service-profile load-balancing- exempt on page 496</td>
</tr>
<tr>
<td></td>
<td>display load-balancing group on page 396</td>
</tr>
<tr>
<td>MAP Administration and</td>
<td>set ap name on page 429</td>
</tr>
<tr>
<td>Maintenance</td>
<td>set ap blink on page 416</td>
</tr>
<tr>
<td></td>
<td>set ap upgrade-firmware on page 444</td>
</tr>
<tr>
<td></td>
<td>set ap force-image- download on page 426</td>
</tr>
<tr>
<td></td>
<td>reset ap on page 410</td>
</tr>
<tr>
<td></td>
<td>set ap radio channel on page 435</td>
</tr>
<tr>
<td></td>
<td>set ap radio tx-power on page 441</td>
</tr>
<tr>
<td></td>
<td>clear ap radio on page 356</td>
</tr>
<tr>
<td></td>
<td>display ap config on page 364</td>
</tr>
<tr>
<td></td>
<td>display ap status on page 379</td>
</tr>
<tr>
<td></td>
<td>display ap counters on page 367</td>
</tr>
<tr>
<td></td>
<td>display ap global on page 393</td>
</tr>
<tr>
<td></td>
<td>display ap connection on page 391</td>
</tr>
</tbody>
</table>
### Table 51  Map Access Point Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>display ap unconfigured</strong> on page 395</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>display ap qos-stats</strong> on page 374</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>display ap etherstats</strong> on page 375</td>
<td></td>
</tr>
<tr>
<td><strong>MAP Local Switching</strong></td>
<td><strong>set ap local-switching mode</strong> on page 427</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>set ap local-switching vlan-profile</strong> on page 428</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>clear ap local-switching vlan-profile</strong> on page 355</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>display ap arp</strong> on page 362</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>display ap fdb</strong> on page 373</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>display ap vlan</strong> on page 385</td>
<td></td>
</tr>
<tr>
<td><strong>WLAN Mesh Services</strong></td>
<td><strong>set ap boot-configuration mesh mode</strong> on page 418</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>set ap boot-configuration mesh psk-phrase</strong> on page 419</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>set ap boot-configuration mesh psk-raw</strong> on page 420</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>set ap boot-configuration mesh ssid</strong> on page 421</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>set service-profile mesh</strong> on page 498</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>set service-profile bridging</strong> on page 485</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>display ap boot-configuration</strong> on page 390</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>display ap mesh-links</strong> on page 377</td>
<td></td>
</tr>
</tbody>
</table>
clear ap local-switching vlan-profile

Clears the VLAN profile that had been applied to an MAP to use with local switching.

Syntax — clear {ap ap-number local-switching vlan-profile

- ap-number — Index value that identifies the MAP on the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

History — A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to a MAP, traffic for the VLANs specified in the VLAN profile is locally switched by the MAP instead of being tunnelled back to a WX. When the VLAN profile is cleared from the MAP, traffic that had been locally switched is tunneled to a WX.

When clearing a VLAN profile causes traffic that had been locally switched by MAPs to be tunneled to a WX, the sessions of clients associated with the MAPs where the VLAN profile is applied are terminated, and the clients must re-associate with the MAPs.

Examples — The following command clears the VLAN profile that had been applied to MAP 7:

WX# clear ap 7 local-switching vlan-profile
success: change accepted.

See Also
- set vlan profile on page 175
- set ap local-switching mode on page 427
- set ap local-switching vlan-profile on page 428
clear ap radio

Disables a MAP radio and resets it to its factory default settings.

**Syntax** — `clear ap ap-num } radio { 1 | 2 | all}

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- `radio all` — All radios on the MAP.

**Defaults** — The `clear ap radio` command resets the radio to the default settings listed in Table 52 and in Table 73 on page 464.

**Table 52** Radio-Specific Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>antennatype</td>
<td>For most MAP models, the default is <code>internal</code>. The default for the 802.11b/g radio on model AP3150 is <code>ANT1060</code>.</td>
<td>External antenna model</td>
</tr>
<tr>
<td>Note: This parameter is configurable only on MAPs that support external antennas.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>max-power</td>
<td>highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower</td>
<td>RF Auto-Tuning settings:</td>
</tr>
<tr>
<td>max-retransmissions</td>
<td>10 percent</td>
<td></td>
</tr>
<tr>
<td>min-client-rate</td>
<td>5.5 Mbps for 802.11b/g; 24 Mbps for 802.11b/g</td>
<td></td>
</tr>
<tr>
<td>channel</td>
<td>802.11b — 6</td>
<td>Number of the channel in which a radio transmits and receives traffic</td>
</tr>
<tr>
<td>802.11a — Lowest valid channel number for the country of operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mode</td>
<td><code>disable</code></td>
<td>Operational state of the radio.</td>
</tr>
</tbody>
</table>
clear ap radio

Access — Enabled

History — Introduced in MSS Version 3.0. Version 6.0 removed the dap option for distributed MAPs.

Usage — When you clear a radio, MSS performs the following actions:

- Clears the transmit power, channel, and external antenna setting from the radio.
- Removes the radio from its radio profile and places the radio in the default radio profile.

This command does not affect the PoE setting.

Examples — The following command disables and resets radio 2 on the MAP access point connected to port 3:

WX1200# clear ap 3 radio 2

See Also

- set ap radio mode on page 439
- set ap radio radio-profile on page 440
- set port type ap on page 145

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radio-profile</td>
<td>None. You must add the radios to a radio profile.</td>
</tr>
<tr>
<td>tx-power</td>
<td>Highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.</td>
</tr>
</tbody>
</table>
clear ap boot-configuration

Removes the static IP address configuration for a Distributed MAP.

Syntax — clear ap boot-configuration apnum

- ap ap-number — Index value that identifies the MAP on the WX.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.2. Version 6.0 removed the dap option.

Usage — When the static IP configuration is cleared for a MAP, and a MAP is rebooted, it uses the standard boot process.

Examples — The following command clears the static IP address configuration for MAP 1.

WX# clear ap 1 boot-configuration
This will clear specified AP devices. Would you like to continue? (y/n) [n]y
success: change accepted.

See Also
- display ap boot-configuration on page 390
- set ap boot-configuration ip on page 417
- set ap boot-configuration switch on page 422
- set ap boot-configuration ip on page 417
- set ap boot-configuration vlan on page 423
clear ap radio load-balancing group

Removes a MAP radio from its load-balancing group.

Syntax

```
clear ap ap-number radio {1 | 2} load-balancing group
```

- **ap ap-number** — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — If an MAP radio has been assigned to an RF load balancing group, you can use this command to remove the MAP radio from the group.

Examples — The following command clears radio 1 on MAP 7 from the load balancing group to which it had been assigned:

```
WX# clear ap 7 radio 1 load-balancing group
```

See Also

- display load-balancing group on page 396
- set ap radio load balancing on page 437
- set load-balancing strictness on page 447
- set ap local-switching mode on page 427
**clear radio-profile**

Removes a radio profile or resets one of the profile’s parameters to its default value.

**Syntax** — `clear radio-profile name [parameter]`

- *name* — Radio profile name.
- *parameter* — Radio profile parameter:
  - `beacon-interval`
  - `countermeasures`
  - `dtim-interval`
  - `frag-threshold`
  - `max-rx-lifetime`
  - `max-tx-lifetime`
  - `preamble-length`
  - `rts-threshold`
  - `service-profile`

For information about these parameters, see the `set radio-profile` commands that use them.

**Defaults** — If you reset an individual parameter, the parameter is returned to the default value listed in Table 73 on page 464.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. `countermeasure` parameter added in Version 4.1. Version 4.2 removes the `long-retry` and `short-retry` parameters that no longer apply to radio profiles.

**Usage** — If you specify a parameter, the setting is reset to its default value. The settings of the other parameters are unchanged and the radio profile remains in the configuration. If you do not specify a parameter, the entire radio profile is deleted from the configuration. All radios that use this profile must be disabled before you can delete the profile.

**Examples** — The following commands disable the radios using radio profile `rp1` and reset the `beaconed-interval` parameter to its default value:

```
WX4400# set radio-profile rp1 mode disable
WX4400# clear radio-profile rp1 beacon-interval
success: change accepted.
```
The following commands disable the radios using radio profile rptest and remove the profile:

```
WX4400# set radio-profile rptest mode disable
WX4400# clear radio-profile rptest
success: change accepted.
```

See Also
- `display radio-profile` on page 398
- `set ap radio radio-profile` on page 440
- `set radio-profile mode` on page 464
- `display radio-profile` on page 398

---

clear service-profile

Removes a service profile or resets one of the profile’s parameters to its default value.

**Syntax** — `clear service-profile name`  
`[soda {agent-directory | failure-page | remediation-acl | success-page | logout-page}]`

- **soda agent-directory** — Resets the directory for Sygate On-Demand (SODA) agent files to the default directory. By default, the directory name for SODA agent files is the same as the service profile name.
- **soda failure-page** — Resets the page that is loaded when a client fails the SODA agent checks. By default, the page is generated dynamically.
- **soda remediation-acl** — Disables use of the specified remediation ACL for the service profile. When no remediation ACL is specified, a client is disconnected from the network when it fails SODA agent checks.
- **soda success-page** — Resets the page loaded when a client passes the checks performed by the SODA agent. By default, the page is generated dynamically.
- **soda logout-page** — Resets the page loaded when a client logs out of the network. By default, the client is disconnected from the network without loading a page.

**Defaults** — None.
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Options added to clear SODA parameters in Version 4.2.

**Usage** — If the service profile is mapped to a radio profile, you must remove it from the radio profile first. (After disabling all radios that use the radio profile, use the `clear radio-profile name service-profile name` command.)

**Examples** — The following commands disable the radios using radio profile `rp6`, remove service-profile `svcprof6` from `rp6`, then clear `svcprof6` from the configuration.

```
WX4400# set radio-profile rp6 mode disable
WX4400# clear radio-profile rp6 service-profile svcprof6
  success: change accepted.
WX4400# clear service-profile svcprof6
  success: change accepted.
```

**See Also**
- `clear radio-profile` on page 360
- `display service-profile` on page 401
- `set radio-profile mode` on page 464

---

display ap arp

Displays the ARP table for a specified MAP.

**Syntax** — `display ap arp ap-number`

- `ap-number` — Index value that identifies the MAP on the WX.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 6.0.
Examples — The following command displays ARP entries for AP 7:

```
WX# display ap arp 7
```

<table>
<thead>
<tr>
<th>Host</th>
<th>HW Address</th>
<th>VLAN</th>
<th>State</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.5.4.51</td>
<td>00:0b:0e:00:04:0c</td>
<td>1</td>
<td>EXPIRED</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>10.5.4.53</td>
<td>00:0b:0e:02:76:f7</td>
<td>1</td>
<td>RESOLVED</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>

Table 53 describes the fields in this display.

**Table 53** Output for display ap arp

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address, hostname, or alias.</td>
</tr>
<tr>
<td>HW Address</td>
<td>MAC address mapped to the IP address, hostname, or alias.</td>
</tr>
<tr>
<td>VLAN</td>
<td>MAC address mapped to the IP address, hostname, or alias.</td>
</tr>
</tbody>
</table>

**State**
- RESOLVING—MSS sent an ARP request for the entry and is waiting for the reply.
- RESOLVED—Entry is resolved.
- EXPIRED—Entry is expired.

**Type**
- DYNAMIC—Entry was learned from network traffic and ages out if unused for longer than the ARP aging timeout.
- LOCAL—Entry for the WX MAC address. Each VLAN has one local entry for the switch MAC address.
- PERMANENT—Entry does not age out and remains in the configuration even following a reboot.
- STATIC—Entry does not age out but is removed after a reboot.

See Also
- set ap local-switching mode on page 427
- set vlan profile on page 175
**display ap config**

Displays global and radio-specific settings for a MAP access point.

**Syntax** — `display ap config [port-list [radio {1 | 2}]]`

- `ap-number` — Index value that identifies the MAP on the WX.
- `radio 1` — Shows configuration information for radio 1.
- `radio 2` — Shows configuration information for radio 2. (This option does not apply to single-radio models.)

**Defaults** — None.

**Access** — All.


**Usage** — MSS lists information separately for each MAP access point.

**Examples** — The following example shows configuration information for MAP 2:

```
WX# display ap config 2
AP 2: serial-id: 123456789, AP model: AP-3750, bias: high, name: AP02
  upgrade-firmware: YES
  force-image-download: NO
  communication timeout: 10
  location:
  contact:
  Radio 1: type: 802.11g, mode: disabled, channel: dynamic
    tx pwr: 18, profile: default
    auto-tune max-power: default,
    load-balance-group: ,
    load-balance-enable: YES,
    force-rebalance: NO,
    local-switching: disabled, vlan-profile: default
```

Table 54 describes the fields in this display.
### Table 54  Output for display ap config

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>WX port number to which the MAP is connected, if specified for the MAP.</td>
</tr>
<tr>
<td>AP</td>
<td>Index number that identifies the MAP to the WX.</td>
</tr>
<tr>
<td>Serial-id</td>
<td>Serial ID of the MAP access point.</td>
</tr>
<tr>
<td>AP model</td>
<td>MAP access point model number.</td>
</tr>
<tr>
<td>bias</td>
<td>Bias of the WX connection to the MAP:</td>
</tr>
<tr>
<td></td>
<td>- High</td>
</tr>
<tr>
<td></td>
<td>- Low</td>
</tr>
<tr>
<td>name</td>
<td>MAP access point name, if configured.</td>
</tr>
<tr>
<td>upgrade-firmware</td>
<td>State of the firmware upgrade option:</td>
</tr>
<tr>
<td></td>
<td>- YES (automatic upgrades are enabled)</td>
</tr>
<tr>
<td></td>
<td>- NO (automatic upgrades are disabled)</td>
</tr>
<tr>
<td>force-image-download</td>
<td>State of the option to force the MAP to download its software image from the WX switch instead of loading the image that is locally stored on the MAP.</td>
</tr>
<tr>
<td>communication</td>
<td></td>
</tr>
<tr>
<td>timeout</td>
<td></td>
</tr>
<tr>
<td>location</td>
<td>Location information for the MAP.</td>
</tr>
<tr>
<td>contact</td>
<td>Contact information for the MAP.</td>
</tr>
<tr>
<td>Radio</td>
<td>Radio number. The information listed below this field applies specifically to the radio.</td>
</tr>
<tr>
<td>type</td>
<td>Radio type:</td>
</tr>
<tr>
<td></td>
<td>- 802.11a</td>
</tr>
<tr>
<td></td>
<td>- 802.11b</td>
</tr>
<tr>
<td></td>
<td>- 802.11g</td>
</tr>
<tr>
<td>mode</td>
<td>Radio state:</td>
</tr>
<tr>
<td></td>
<td>- Enabled</td>
</tr>
<tr>
<td></td>
<td>- Disabled</td>
</tr>
<tr>
<td>channel</td>
<td>Channel number.</td>
</tr>
<tr>
<td>antennatype</td>
<td>External antenna model, if applicable.</td>
</tr>
<tr>
<td>tx pwr</td>
<td>Transmit power, in dBm.</td>
</tr>
</tbody>
</table>
Radio profile that manages the radio. Until you assign the radio to a radio profile, MSS assigns the radio to the default radio profile.

- **auto-tune max-power**
  - Maximum power level the RF Auto-Tuning feature can set on the radio.
  - The value *default* means RF Auto-Tuning can set the power up to the maximum level allowed for the country of operation.
  - A specific numeric value means you or another administrator set the maximum value.

- **load-balance-group**
  - Names of the RF load-balancing groups to which the MAP access point belongs. If the value is *None*, the access point does not belong to any load balancing groups.
  - **Note:** This field is displayed only if the MAP is a member of a group.

- **load-balance-enable**
  - Whether RF load balancing is enabled for this MAP.

- **force-rebalance**
  - Whether the MAP radio to disassociates its client sessions and rebalance them whenever a new MAP radio is added to the RF load balancing group.

- **local-switching**
  - Whether local packet switching is enabled for the MAP.

- **vlan-profile**
  - The VLAN profile the MAP uses for local packet switching, indicating which VLANs are locally switched.

### See Also
- `display ap connection` on page 391
- `display ap global` on page 393
- `display ap unconfigured` on page 395
- `display radio-profile` on page 398
- `set ap` on page 135
- `set port type ap` on page 145
- `set ap bias` on page 415
- `set ap group` on page 427
- `set ap name` on page 429
- `set ap upgrade-firmware` on page 444
display ap counters

Displays MAP access point and radio statistics counters.

Syntax — display ap counters [ap-number[radio {1 | 2}]]

- **ap-number** — Index value that identifies the MAP on the WX.
- **radio 1** — Shows statistics counters for radio 1.
- **radio 2** — Shows statistics counters for radio 2. (This option does not apply to single-radio models.)

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0. New fields added in MSS Version 4.0:

- Radio Recv Phy Err Ct
- Transmit Retries
- Radio Adjusted Tx Pwr
- Noise Floor
- 802.3 Packet Tx Ct
- 803.3 Packet Rx Ct
- No Receive Descriptor

Version 6.0 removed the *dap* option and added the Illegal Rates field.

**Usage** — To display statistics counters and other information for individual user sessions, use the *display sessions network* command.
Examples — The following command shows statistics counters for Distributed MAP 7:

```
WX1200# display ap counters 7
AP: 7 radio: 1
==================================
LastPktXferRate        2 PktTxCount         91594255
NumCntInPwrSave        4294967683 MultiPktDrop       0
LastPktRxSigStrength   -54 MultiByteDrop       0
LastPktSigNoiseRatio   40 User Sessions      5
TKIP Pkt Transfer Ct   0 MIC Error Ct       0
TKIP Pkt Replays       0 TKIP Decrypt Err  0
CCMP Pkt Decrypt Err   0 CCMP Pkt Replays  0
CCMP Pkt Transfer Ct   0 RadioResets       0
Radio Recv Phy Err Ct  0 Transmit Retries  60501
Radio Adjusted Tx Pwr 15 Noise Floor       -93
802.3 Packet Tx Ct    0 802.3 Packet Rx Ct 0
No Receive Descriptor  0 Illegal Rates    2

|           |         |           |           |           |
|-----------|---------|-----------|-----------|
| TxUnipkt  | TxUniByte| RxPkt     | RxBYTE    | UndcrptPkt| UndcrptByte|
| TxMultiPkt| TxMultiByte|           |           |           |
| PhyError  |         |           |           |           |
| 1.0:      | 1644920 | 9631741   | 405041    | 8913512   | 0 0 13963  |
| 2.0:      | 603     | 248716    | 191103    | 4608065   | 0 0 30547  |
| 5.5:      | 370594  | 52742     | 27616521  | 4445625   | 2427 133217 0 0 723 |
| 6.0:      | 0       | 0         | 0         | 0         | 0 0 51    |
| 9.0:      | 0       | 0         | 0         | 1         | 172 0 0   53   |
| 11.0:     | 8016    | 2590353   | 85479     | 3897587   | 0 0 1195  |
| 12.0:     | 0       | 0         | 0         | 0         | 0 0 26    |
| 18.0:     | 0       | 0         | 0         | 0         | 0 0 38    |
| 24.0:     | 0       | 0         | 0         | 0         | 0 0 47    |
| 36.0:     | 0       | 0         | 0         | 0         | 0 0 1     |
| 48.0:     | 0       | 0         | 0         | 1         | 68 0 0    29   |
| 54.0:     | 0       | 0         | 0         | 0         | 0 0 5     |

TOTL: 543705 52742 40087331 4445625 684050 17552381 0 0 46441
Table 55 describes the fields in this display.

**Table 55  Output for display ap counters**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Distributed MAP number.</td>
</tr>
<tr>
<td>Port</td>
<td>WX port number (if the MAP is directly connected to the WX and the WX port is configured as a MAP access point).</td>
</tr>
<tr>
<td>radio</td>
<td>Radio number.</td>
</tr>
<tr>
<td>LastPktXferRate</td>
<td>Data transmit rate, in Mbps, of the last packet received by the MAP access point.</td>
</tr>
<tr>
<td>NumCntInPwrSave</td>
<td>Number of clients currently in power save mode.</td>
</tr>
<tr>
<td>LastPktRxSigStrength</td>
<td>Signal strength, in dBm, of the last packet received by the MAP access point.</td>
</tr>
<tr>
<td>LastPktSigNoiseRatio</td>
<td>Signal-to-noise ratio, in decibels (dB), of the last packet received by the MAP access point.</td>
</tr>
<tr>
<td></td>
<td>This value indicates the strength of the radio signal above the noise floor. For example, if the noise floor is -88 and the signal strength is -68, the SNR is 20.</td>
</tr>
<tr>
<td></td>
<td>If the value is below 10, this indicates a weak signal and might indicate a problem in the RF environment.</td>
</tr>
<tr>
<td>TKIP Pkt Transfer Ct</td>
<td>Total number of TKIP packets sent and received by the radio.</td>
</tr>
<tr>
<td>TKIP Pkt Replays</td>
<td>Number of TKIP packets that were resent to the MAP by a client.</td>
</tr>
<tr>
<td></td>
<td>A low value (under about one hundred) does not necessarily indicate a problem. However, if this counter is increasing steadily or has a very high value (in the hundreds or more), a Denial of Service (DoS) attack might be occurring. Contact 3Com TAC.</td>
</tr>
<tr>
<td>CCMP Pkt Decrypt Err</td>
<td>Number of times a decryption error occurred with a packet encrypted with CCMP.</td>
</tr>
<tr>
<td></td>
<td>Occasional decryption errors do not indicate a problem. However, steadily increasing errors or a high number of errors can indicate that data loss is occurring in the network. Generally, this is caused by a key mismatch between a client and the MAP. To locate the client that is experiencing decryption errors (and therefore is likely causing this counter to increment on the MAP), use the <strong>display sessions network session-id session-id</strong> command for each client on the radio. After you identify the client that is causing the errors, disable and reenable the client (wireless NIC).</td>
</tr>
</tbody>
</table>
### Table 55  Output for display ap counters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCMP Pkt Transfer Ct</td>
<td>Total number of CCMP packets sent and received by the radio.</td>
</tr>
<tr>
<td>Radio Recv Phy Err Ct</td>
<td>Number of times radar caused packet errors. If this counter increments rapidly, there is a problem in the RF environment. This counter increments only when radar is detected. Rate-specific Phy errors are instead counted in the PhyError columns for individual data rates.</td>
</tr>
<tr>
<td>Radio Adjusted Tx Pwr</td>
<td>Current power level set on the radio. If RF Auto-Tuning of power is enabled, this value is the power set by RF Auto-Tuning. If RF Auto-Tuning is disabled, this value is the statically configured power level.</td>
</tr>
<tr>
<td>802.3 Packet Tx Ct</td>
<td>Number of raw 802.3 packets transmitted by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.</td>
</tr>
<tr>
<td>No Receive Descriptor</td>
<td>Number of packets for which the MAP could not create a descriptor. A descriptor describes a received packet’s size and its location in MAP memory. The MAP buffers descriptors, and clears them during interframe spaces. This counter increments if the MAP runs out of buffers for received packets. This condition can occur when a noise burst temporarily floods the air and the MAP attempts to buffer the noise as packets. Buffer overruns are normal while a MAP is booting. However, if they occur over an extended period of time when the MAP is fully active, this can indicate RF interference.</td>
</tr>
<tr>
<td>Illegal Rates</td>
<td>Number of times a client attempted to connect with a disabled data rate.</td>
</tr>
<tr>
<td>PktTxCount</td>
<td>Number of packets transmitted by the radio.</td>
</tr>
<tr>
<td>MultiPktDrop</td>
<td>Number of multicast packets dropped by the radio due to a buffer overflow on the MAP. This counter increments if there is too much multicast traffic or there is a problem with the multicast packets. Normally, this counter should be 0.</td>
</tr>
<tr>
<td>MultiBytDrop</td>
<td>Number of multicast bytes dropped by the radio due to a buffer overflow on the MAP. (See the description for MultiPktDrop.)</td>
</tr>
</tbody>
</table>
User Sessions

Number of clients currently associated with the radio. Generally, this counter is equal to the number of sessions listed for the radio in display sessions output. However, the counter can differ from the counter in display sessions output if a client is associated with the radio but has not yet completed 802.1X authentication. In this case, the client is counted by this counter but not in the display sessions output.

Although there is no specific normal range for this counter, a high or low number relative to other radios can mean the radio is underutilized or overutilized relative to the other radios. (However, if the clients are VoIP phones, a relatively high number of clients does not necessarily mean overutilization since voice clients consume less bandwidth on average than data clients.)

MIC Error Ct

Number of times the radio received a TKIP-encrypted frame with an invalid MIC. Normally, the value of this counter should always be 0. If the value is not 0, check the system log for MIC error messages and contact 3Com TAC.

TKIP Decrypt Err

Number of times a decryption error occurred with a packet encrypted with TKIP. (See the description for CCMP Pkt Decrypt Err.)

CCMP Pkt Replays

Number of CCMP packets that were resent to the MAP by a client. (See the description for TKIP Pkt Replays.)

RadioResets

Number of times the radio has been reset. Generally, a reset occurs as a result of RF noise. It is normal for this counter to increment a few times per day.

Transmit Retries

Number of times the radio retransmitted a unicast packet because it was not acknowledged. The MAP uses this counter to adjust the transmit data rate for a client, in order to minimize retries.

The ratio of transmit retries to transmitted packets (TxUniPkt) indicates the overall transmit quality. A ratio of about 1 retry to 10 transmitted packets indicates good transmit quality. A ratio of 3 or more to 10 indicates poor transmit quality.

This counter includes unacknowledged probes. Some clients do not respond to probes, which can make this counter artificially high.
### Table 55  Output for display ap counters (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noise Floor</td>
<td>Received signal strength at which the MAP can no longer distinguish 802.11 packets from ambient RF noise. A value around -90 or higher is good for an 802.11b/g radio. A value around -80 or higher is good for an 802.11a radio. Values near 0 can indicate RF interference.</td>
</tr>
<tr>
<td>802.3 Packet Rx Ct</td>
<td>Number of raw 802.3 packets received by the radio. These are LocalTalk (AppleTalk) frames. This counter increments only if LocalTalk traffic is present.</td>
</tr>
<tr>
<td>TxUniPkt</td>
<td>Number of unicast packets transmitted by the radio.</td>
</tr>
<tr>
<td>TxMultiPkt</td>
<td>Number of multicast packets transmitted by the radio.</td>
</tr>
<tr>
<td>TxUniByte</td>
<td>Number of unicast bytes transmitted by the radio.</td>
</tr>
<tr>
<td>TxMultiByte</td>
<td>Number of multicast bytes transmitted by the radio.</td>
</tr>
<tr>
<td>RxPkt</td>
<td>Number of packets received by the radio.</td>
</tr>
<tr>
<td>RxByte</td>
<td>Number of bytes received by the radio.</td>
</tr>
<tr>
<td>UndcryptedPkt</td>
<td>Number of undecryptable packets received by the radio. It is normal for this counter to increment even in stable networks and does not necessarily indicate an attack. For example, a client might be sending incorrect key information. However, if the counter increments rapidly, there might be a problem in the network.</td>
</tr>
<tr>
<td>UndcryptedByte</td>
<td>Number of undecryptable bytes received by the radio. (See the description for UndcrptPkt.)</td>
</tr>
<tr>
<td>PhyError</td>
<td>Number of packets that could not be decoded by the MAP. This condition can have any of the following causes:</td>
</tr>
<tr>
<td></td>
<td>• Collision of an 802.11 packet.</td>
</tr>
<tr>
<td></td>
<td>• Packet whose source is too far away, thus rendering the packet unintelligible by the time it reaches the MAP.</td>
</tr>
<tr>
<td></td>
<td>• Interference caused by an 802.11b/g phone or other source.</td>
</tr>
<tr>
<td></td>
<td>It is normal for this counter to be about 10 percent of the total RxByte count. It is also normal for higher data rates to have higher Phy error counts than lower data rates.</td>
</tr>
</tbody>
</table>
**display ap fdb**

Displays the entries in a specified AP’s forwarding database.

**Syntax** — `display ap fdb ap-number`

- *ap-number* — Index value that identifies the MAP on the WX.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 6.0.

**Examples** — The following command displays FDB entries for AP 7:

```
WX# display ap fdb 7
AP 7:
# = System Entry. $ = Authenticate Entry
VLAN  TAG  Dest MAC/Route Des [CoS]  Destination Ports
----  ---  ------------------ ----- -----------------
 4095 4095 00:0b:0e:00:ca:c1 # CPU
 4095   0  00:0b:0e:00:04:0c     eth0
```

Table 56 describes the fields in the **display ap fdb** output.

**Table 56**  Output for display ap fdb

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>TAG</td>
<td>VLAN tag value. If the interface is untagged, the TAG field is blank.</td>
</tr>
<tr>
<td>Dest MAC/Route Des</td>
<td>MAC address of this forwarding entry is destination.</td>
</tr>
<tr>
<td>CoS</td>
<td>Type of entry. The entry types are explained in the first row of the command output.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This Class of Service (CoS) value is not associated with MSS quality of service (QoS) features.</td>
</tr>
<tr>
<td>Destination Ports</td>
<td>WX switch port associated with the entry. A switch sends traffic to the destination MAC address through this port.</td>
</tr>
</tbody>
</table>
See Also
- set ap local-switching mode on page 427
- set vlan profile on page 175

**display ap qos-stats** Displays statistics for MAP forwarding queues.

**Syntax** — display ap qos-stats [ap-number] [clear]

- **ap-number** — Index value that identifies the MAP on the WX.
- **clear** — Clears the counters after displaying their current values.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0. Version 4.2 added the TxDrop field. Version 6.0 removed the dap option.

**Usage** — Repeating this command with the clear option at regular intervals allows you to monitor transmission and drop rates.

**Examples** — The following command shows statistics for the MAP forwarding queues on a Distributed MAP.

```
WX4400# display ap qos-stats 4
CoS   Queue      Tx         TxDrop
======================================
  AP: 4 radio: 1
  1,2  Background 0 0
  0,3  BestEffort 15327 278
  4,5  Video 0 0
  6,7  Voice 1714881 0
  AP: 4 radio: 2
  1,2  Background 0 0
  0,3  BestEffort 0 0
  4,5  Video 0 0
  6,7  Voice 0 0
```
Table 57 describes the fields in this display.

**Table 57  Output for display ap qos-stats**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS</td>
<td>CoS value associated with the forwarding queues.</td>
</tr>
<tr>
<td>Queue</td>
<td>Forwarding queue.</td>
</tr>
<tr>
<td>AP</td>
<td>Distributed MAP number or MAP port number.</td>
</tr>
<tr>
<td>radio</td>
<td>Radio number.</td>
</tr>
<tr>
<td>Tx</td>
<td>Number of packets transmitted to the air from the queue.</td>
</tr>
<tr>
<td>TxDrop</td>
<td>Number of packets dropped from the queue instead of being transmitted.</td>
</tr>
</tbody>
</table>

Some packet drops are normal, especially if the RF environment is noisy. Also, it is normal for a mildly congested radio to drop low-priority packets proportionally more often than high-priority packets. However, continuous packet drops from the Voice queue can indicate over-subscription or excessive interference in the RF environment.

**display ap etherstats**

Displays Ethernet statistics for an Ethernet port on a MAP.

**Syntax** — `display ap etherstats ap-number`

- `ap-number` — Index value that identifies the MAP on the WX.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
**Examples** — The following command displays Ethernet statistics for the Ethernet ports on Distributed MAP 1:

```markdown
WX4400# display ap etherstats 1
AP: 1                ether: 1
=================================
RxUnicast:          75432   TxGoodFrames:       55210
RxMulticast:        18789   TxSingleColl:       32
RxBroadcast:         8      TxLateColl:         0
RxGoodFrames:       94229   TxMaxColl:          0
RxAlignErrs:         0      TxMultiColl:         47
RxShortFrames:       0      TxUnderruns:        0
RxCrcErrors:         0      TxCarrierLoss:      0
RxOverruns:          0      TxDeferred:         150
RxDiscards:          0
```

Table 58 describes the fields in this display.

**Table 58  Output of display ap etherstats**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RxUnicast</td>
<td>Number of unicast frames received.</td>
</tr>
<tr>
<td>RxMulticast</td>
<td>Number of multicast frames received.</td>
</tr>
<tr>
<td>RxBroadcast</td>
<td>Number of broadcast frames received.</td>
</tr>
<tr>
<td>RxGoodFrames</td>
<td>Number of frames received properly from the link.</td>
</tr>
<tr>
<td>RxAlignErrs</td>
<td>Number of received frames that were both misaligned and contained a CRC error.</td>
</tr>
<tr>
<td>RxShortFrames</td>
<td>Number of received frames that were shorter than the minimum frame length.</td>
</tr>
<tr>
<td>RxCrcErrors</td>
<td>Number of received frames that were discarded due to CRC errors.</td>
</tr>
<tr>
<td>RxOverruns</td>
<td>Number of frames known to be lost due to a temporary lack of hardware resources.</td>
</tr>
<tr>
<td>RxDiscards</td>
<td>Number of frames known to be lost due to a temporary lack of software resources.</td>
</tr>
<tr>
<td>TxGoodFrames</td>
<td>Number of frames transmitted properly on the link.</td>
</tr>
<tr>
<td>TxSingleColl</td>
<td>Number of transmitted frames that encountered a single collision.</td>
</tr>
<tr>
<td>TxAgeLateColl</td>
<td>Number of frames that were not transmitted because they encountered a collision outside the normal collision window.</td>
</tr>
</tbody>
</table>
display ap group

Deprecated in MSS Version 6.0. To display information about RF load balancing, see “display load-balancing group” on page 396.

display ap mesh-links

Displays information about the links an MAP has to Mesh APs and Mesh Portal APs.

Syntax — display ap mesh-links ap-number [path]

- **ap-number** — Index value that identifies the MAP on the WX.
- **path** — Displays statistics for the path of mesh services devices of which this MAP is part.

Defaults — None.

Access — All.

History — Introduced in MSS Version 6.0.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TxMaxColl</td>
<td>Number of frames that were not transmitted because they encountered the maximum allowed number of collisions. Typically, this occurs only during periods of heavy traffic on the network.</td>
</tr>
<tr>
<td>TxMultiColl</td>
<td>Number of transmitted frames that encountered more than one collision.</td>
</tr>
<tr>
<td>TxUnderruns</td>
<td>Number of frames that were not transmitted or retransmitted due to temporary lack of hardware resources.</td>
</tr>
<tr>
<td>TxCarrierLoss</td>
<td>Number of frames transmitted despite the detection of a deassertion of CRS during the transmission.</td>
</tr>
<tr>
<td>TxDeferred</td>
<td>Number of frames deferred before transmission due to activity on the link.</td>
</tr>
</tbody>
</table>

---

**Table 58** Output of display ap etherstats (continued)
Examples — The following command mesh link information for AP 7:

WX# display ap mesh-links 7
AP: 7 IP-addr: 1.1.1.3
Operational Mode: Mesh-Portal
Downlink Mesh-APs

BSSID: 00:0b:0e:17:bb:3f (54 Mbps)

<table>
<thead>
<tr>
<th></th>
<th>packets</th>
<th>bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>TX</td>
<td>307</td>
<td>44279</td>
</tr>
<tr>
<td>RX</td>
<td>315</td>
<td>215046</td>
</tr>
</tbody>
</table>

The following command displays statistics for the path of mesh services devices that MAP is part of.

WX# display ap mesh-links 7 path
Status Flags:
m - Mesh AP, p - Mesh Portal, b - Bridging
AP Current Uplink Uplink Uplink Packets
Num Status AP RSN RX TX

0007 ---- -

Table 59 describes the fields in the display ap mesh-links output.

Table 59 Output for display ap mesh-links

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Identifier for the MAP on the WX switch.</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name</td>
</tr>
<tr>
<td>IP-addr</td>
<td>IP address of the MAP.</td>
</tr>
<tr>
<td>Operational Mode</td>
<td>Whether this MAP is a Mesh AP or a Mesh Portal AP</td>
</tr>
<tr>
<td></td>
<td>Downlink Mesh-APs Information about the Mesh APs for which this MAP is a Mesh Portal MAP.</td>
</tr>
<tr>
<td>Downlink Mess-APs</td>
<td>Information about the Mesh APs for which this MAP is a Mesh Portal MAP.</td>
</tr>
<tr>
<td>BSSID</td>
<td>The BSSID of the Mesh AP.</td>
</tr>
<tr>
<td>TX</td>
<td>The amount of traffic (packets and bytes) transmitted to the Mesh AP.</td>
</tr>
<tr>
<td>RX</td>
<td>The amount of traffic (packets and bytes) received from the Mesh AP.</td>
</tr>
</tbody>
</table>
display ap status

Displays MAP access point and radio status information.

**Syntax** — display ap status [terse] [ap-number | all [radio {1 | 2}]]

- **terse** — Displays a brief line of essential status information for each MAP.
- **ap-number** — Index value that identifies the MAP on the WX.
- **all** — Shows status information for all directly attached MAP access points and all Distributed MAP access points configured on the switch.
- **radio 1** — Shows status information for radio 1.
- **radio 2** — Shows status information for radio 2. (This option does not apply to single-radio models.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. True base MAC addresses of radios are displayed in MSS Version 3.2. Previously, the base MAC address displayed for a radio was the true base MAC address plus 2. Note that a radio’s base MAC address is also used as the BSSID of the first SSID configured on the radio. New option added: terse; new option added for display ap status: all; new field added: fingerprint; MAP-WX security status added to State field in MSS Version 4.0. External antenna information added after the radio state information, to indicate when an antenna has been detected and to indicate the configured antenna model number; auto flag added to indicate operational channel or power settings that are configured by RF Auto-Tuning in MSS Version 4.1. Version 4.2 added Radar Scan and Radar Detected flags to indicate when the Dynamic Frequency Selection (DFS) feature is scanning for radar or has stopped transmitting due to detected radar. The flags apply to 802.11a radios only, and only for country codes where DFS is used.

Version 6.0 removed the dap option.

See Also

- set ap boot-configuration mesh ssid on page 421
- set service-profile mesh on page 498
Examples — The following command displays the status of a MAP access point:

WX4400# display ap status 7
Dap: 1, IP-addr: 10.2.34.56 (vlan 'vlan-corp'), MAP model: AP2750,
    manufacturer: 3Com, name: DAP01

=====================================================
State:     operational
CPU info:  IBM:PPC speed=266666664 Hz version=405GPr
    id=0x28f10158a47f0408 ram=33554432
    s/n=0332600444 hw_rev=A3
Uptime:    21 hours, 27 minutes, 51 seconds
Radio 1 type: 802.11g, state: configure succeed [Enabled]
    operational channel: 64 operational power: 14
    base mac: 00:0b:0e:00:d2:c1
    bssid1: 00:0b:0e:00:d2:94, ssid: private

The following command displays the status of a directly connected MAP:

WX# display ap status 7
AP: 7, AP model: AP3750, manufacturer 3Com, name: MP07

=====================================================
State: operational (not encrypt)
CPU info: IBM:PPC speed=266666664 Hz version=405GPr, ram=33554432
    s/n=0333703050 hw_rev=A3
Uptime: 503 hours, 51 minutes, 5 seconds
Radio 1 type: 802.11g, state: configure succeed [Enabled]
    operational channel: 11 (Auto) operational power: 1
    bssid1: 00:0b:0e:00:ca:c0, ssid: public
    bssid2: 00:0b:0e:00:ca:c2, ssid: employee-net
    load balance: enabled, current load: (unavailable)
RFID Reports: Inactive
Radio 2 type: 802.11a, state: configure succeed [Disabled] (Sweep mode)
    operational channel: 44 (Auto) operational power: 1
    bssid1: 00:0b:0e:00:ca:c1, ssid: mycorp-tkip
    load balance: enabled, current load: (unavailable)
RFID Reports: Inactive
The following command uses the `terse` option to display brief information for MAPs:

```
WX# display ap status terse
Total number of entries: 120
Operational: 1, Image Downloading: 0, Unknown: 119, Other: 0
Flags: o = operational, b = booting, d = image downloading
       c = configuring, f = configuration failed
       a = auto AP, m = mesh AP, p = mesh portal
       i = insecure, e = encrypted, u = unencrypt
AP Flag IP Address Model MAC Address Radio1 Radio2 Uptime
--- ---- --------------- --------- ----------------- ------ ------ ------
 7 o--u AP3750 00:0b:0e:00:ca:c0 D11/1 D44/1 21d00h
```

Table 60 and Table 61 describe the fields in this display.

### Table 60  Output for display ap status

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Connection ID for the Distributed MAP.</td>
</tr>
<tr>
<td>Port</td>
<td>WX port number.</td>
</tr>
<tr>
<td>IP-addr</td>
<td>IP address of the MAP. The address is assigned to the MAP by a DHCP server.</td>
</tr>
<tr>
<td>AP model</td>
<td>MAP access point model number.</td>
</tr>
<tr>
<td>manufacturer</td>
<td>Company that made the MAP access point.</td>
</tr>
<tr>
<td>fingerprint</td>
<td>Hexadecimal fingerprint of the MAP’s public encryption key.</td>
</tr>
<tr>
<td>name</td>
<td>MAP access point name.</td>
</tr>
<tr>
<td>Link</td>
<td>Status of this link with the MAP access point and the MAP port at the other end of the link. The status can be up or down.</td>
</tr>
<tr>
<td>MAP port</td>
<td>MAP port number connected to this WX port.</td>
</tr>
</tbody>
</table>
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

State of the MAP:

- **init** — The MAP has been recognized by the WX but has not yet begun booting.
- **booting** — The MAP has asked the WX for a boot image.
- **image downloading** — The MAP is receiving a boot image from the WX.
- **image downloaded** — The MAP has received a boot image from the WX and is booting.
- **configuring** — The MAP has booted and is ready to receive or is already receiving configuration parameters from the WX.
- **operational** — The MAP has received configuration parameters for one or more radios and is ready to accept client connections.
- **configure failure** — One or more of the radio parameters received from the WX is invalid.

For Distributed MAPs, this field also indicates whether the MAP management traffic with the WX is encrypted, and whether the MAP’s fingerprint has been verified on the WX:

- **not encrypted** — The management session is not encrypted.
- **encrypted but fingerprint not verified** — The MAP management traffic is encrypted, but the MAP fingerprint has not been verified in MSS.
- **encrypted and verified** — The MAP management traffic is encrypted and the MAP fingerprint has been verified in MSS.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>State of the MAP:</td>
</tr>
<tr>
<td></td>
<td>- <strong>init</strong> — The MAP has been recognized by the WX but has not yet begun booting.</td>
</tr>
<tr>
<td></td>
<td>- <strong>booting</strong> — The MAP has asked the WX for a boot image.</td>
</tr>
<tr>
<td></td>
<td>- <strong>image downloading</strong> — The MAP is receiving a boot image from the WX.</td>
</tr>
<tr>
<td></td>
<td>- <strong>image downloaded</strong> — The MAP has received a boot image from the WX and is booting.</td>
</tr>
<tr>
<td></td>
<td>- <strong>configuring</strong> — The MAP has booted and is ready to receive or is already receiving configuration parameters from the WX.</td>
</tr>
<tr>
<td></td>
<td>- <strong>operational</strong> — The MAP has received configuration parameters for one or more radios and is ready to accept client connections.</td>
</tr>
<tr>
<td></td>
<td>- <strong>configure failure</strong> — One or more of the radio parameters received from the WX is invalid.</td>
</tr>
</tbody>
</table>

CPU info

Specifications and identification of the CPU.

Uptime

Amount of time since the MAP last rebooted using this link.

**Note:** This field is displayed only when this link is the MAP access point’s primary link.
Radio 1 type  802.11 type and configuration state of the radio.

Radio 2 type
  - The *configure succeed* state indicates that the MAP has received configuration parameters for the radio and the radio is ready to accept client connections.
  
  - *802.11b protect* indicates that the 802.11b/g radio is sending messages to 802.11b devices, while sending 802.11g traffic at higher data rates, to inform the 802.11b devices about the 802.11g traffic and reserve bandwidth for the traffic. Protection mode remains in effect until 60 seconds after the last 802.11b traffic is detected by the 802.11b/g radio.

  - *Sweep Mode* indicates that a disabled radio is nonetheless participating in rogue detection scans. Even though this message appears only for disabled radios, all radios, enabled or disabled, participate in rogue detection.

  - *Countermeasures Enabled* indicates that the radio is sending countermeasures packets to combat a rogue.

  - *Radar Scan* indicates that the radio is performing the initial channel availability check for Dynamic Frequency Selection (DFS). This state lasts during the first 60 seconds an 802.11a radio is on a new channel, during which time the radio does not transmit. If the radio does not detect any radar on the channel, the radio starts using the channel for data. If the radio does detect radar, the flag changes to *Radar Detected*. (See below).

  - *Radar Detected* indicates that DFS has detected radar on the channel. When this occurs, the MAP stops transmitting on the channel for 30 minutes. If RF Auto-Tuning is enabled for channel assignment, the radio selects another channel and performs the initial channel availability check on the new channel, during which time the flag changes back to *Radar Scan*.

*Note:* *Radar Scan* and *Radar Detected* apply only to 802.11a radios, for country codes that use DFS.
The following information appears for external antennas:

- **External antenna detected, configured as antenna-model**—Indicates that an external antenna has been detected, and lists the antenna model configured on the radio. (MSS does not detect the specific model.)

- **External antenna detected, not configured**—Indicates that an external antenna was detected but no external antenna is configured on the radio.

- **External antenna not detected, configured as antenna-model**—Indicates that an external antenna is configured on the radio but no external antenna was detected.

---

**Table 60** Output for display ap status (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio 1 type</td>
<td></td>
</tr>
<tr>
<td>Radio 2 type</td>
<td></td>
</tr>
<tr>
<td>(cont.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The following information appears for external antennas:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Operational channel</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the channel number is followed by (Auto), the value was set by RF Auto-Tuning.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Operational power</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the power setting is followed by (Auto), the value was set by RF Auto-Tuning.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Base mac</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>BSSID, SSID</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Load balance</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Current load</strong></td>
</tr>
</tbody>
</table>

---

**Table 61** Output for display ap status terse

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>The number of the MAP connected.</td>
</tr>
<tr>
<td>Flag</td>
<td>Operational status flags for the MAP.</td>
</tr>
<tr>
<td></td>
<td>For flag definitions, see the key in the command output.</td>
</tr>
<tr>
<td>Port</td>
<td>WX port number connected to the MAP.</td>
</tr>
<tr>
<td>Flg</td>
<td>Operational status flags for the MAP.</td>
</tr>
<tr>
<td></td>
<td>For flag definitions, see the key in the command output.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the MAP. The address is assigned to the MAP by a DHCP server.</td>
</tr>
<tr>
<td></td>
<td>This field is applicable only if the MAP is configured on the WX switch as a Distributed MAP.</td>
</tr>
</tbody>
</table>
**display ap vlan**

Displays information about the VLANs that are either locally switched by the specified MAP or tunneled from the MAP to an WX switch.

**Syntax** — `display ap vlan ap-number`

- `ap-number` — Index value that identifies the MAP on the WX.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 6.0.

**Examples** — The following command displays information about the VLANs switched by AP 7:

```plaintext
WX# display ap vlan 7
AP 7:
VLAN Name  Mode Port Tag
--- ------ ----- ----
1 default  local   1  none
2 red      local   1  2
            radio_1 20
            radio_1 21
            radio_2 22
4 green    local   1  4
            radio_1 23
5 yellow   tunnel  wx_tun 5
            radio_1 24
```
Table 62 describes the fields in the `display ap vlan` output.

**Table 62  Output for display ap vlan**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>Name</td>
<td>VLAN name</td>
</tr>
<tr>
<td>Mode</td>
<td>Whether packets for the VLAN are locally switched by the MAP, or are tunneled to an WX switch, which places them on the VLAN.</td>
</tr>
<tr>
<td>Port</td>
<td>The port(s) through which traffic for the VLAN is sent.</td>
</tr>
<tr>
<td>TAG</td>
<td>VLAN tag value. If the interface is untagged, none is displayed in the TAG field.</td>
</tr>
</tbody>
</table>

**See Also**
- `set ap local-switching mode` on page 427
- `set vlan profile` on page 175

**display auto-tune attributes**

Displays the current values of the RF attributes RF Auto-Tuning uses to decide whether to change channel or power settings.

**Syntax** — `display auto-tune attributes [ap ap-number [radio {1 | 2 | all}]]`

- `ap-number` — Index value that identifies the MAP on the WX.
- `radio 1` — Shows RF attribute information for radio 1.
- `radio 2` — Shows RF attribute information for radio 2. (This option does not apply to single-radio models.)
- `radio all` — Shows RF attribute information for both radios.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 6.0 removed the `dap` option.
Examples — The following command displays RF attribute information for radio 1 on the directly connected MAP access point on port 2:

```
WX1200# display auto-tune attributes ap 2 radio 1
Auto-tune attributes for port 2 radio 1:
  Noise:               -92  Packet Retransmission Count:          0
  Utilization:        0.00  Phy Errors Count:                     0
  CRC Errors count:  122
```  

Table 63 describes the fields in this display.

### Table 63  Output for display auto-tune attributes

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noise</td>
<td>Noise threshold on the active channel. RF Auto-Tuning prefers channels with low noise levels over channels with higher noise levels.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Number of multicast packets per second that a radio can send on a channel while continuously sending fixed size frames over a period of time. The number of packets that are successfully transmitted indicates how busy the channel is.</td>
</tr>
<tr>
<td>CRC Errors count</td>
<td>Number of frames received by the radio on that active channel that had CRC errors. A high CRC error count can indicate a hidden node or co-channel interference.</td>
</tr>
<tr>
<td>Packet Retransmission Count</td>
<td>Number of retransmitted packets sent from the client to the radio on the active channel. Retransmissions can indicate that the client is not receiving ACKs from the MAP radio.</td>
</tr>
<tr>
<td>Phy Errors Count</td>
<td>Number of frames received by the MAP radio that had physical layer errors on the active channel. Phy errors can indicate interference from a non-802.11 device.</td>
</tr>
</tbody>
</table>

See Also

- display auto-tune neighbors on page 388
- display radio-profile on page 398
- set ap radio auto-tune max-power on page 432
- set ap radio auto-tune max-retransmissions on page 433
- set radio-profile auto-tune channel-config on page 450
- set radio-profile auto-tune channel-holddown on page 451
- set radio-profile auto-tune channel-interval on page 452
- set radio-profile auto-tune power-config on page 454
- set radio-profile auto-tune power-interval on page 455
**display auto-tune neighbors**

Displays the other 3Com radios and third-party 802.11 radios that a 3Com radio can hear.

**Syntax** — display auto-tune neighbors

```
[ap map-num [radio {1 | 2 | all}]]
```

**Syntax** — display auto-tune neighbors

```
[ap ap-number [radio {1 | 2 | all}]]
```

- **ap-number** — Index value that identifies the MAP on the WX.
- **radio 1** — Shows neighbor information for radio 1.
- **radio 2** — Shows neighbor information for radio 2. (This option does not apply to single-radio models.)
- **radio all** — Shows neighbor information for both radios.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 6.0 removed the **dap** option.

**Usage** — For simplicity, this command displays a single entry for each 3Com radio, even if the radio is supporting multiple BSSIDs. However, BSSIDs for third-party 802.11 radios are listed separately, even if a radio is supporting more than one BSSID.

Information is displayed for a radio if the radio sends beacon frames or responds to probe requests. Even if a radio SSIDs are unadvertised, 3Com radios detect the empty beacon frames (beacon frames without SSIDs) sent by the radio, and include the radio in the neighbor list.
Examples — The following command displays neighbor information for radio 1 on the directly connected MAP access point on port 2:

WX1200# **display auto-tune neighbors ap 2 radio 1**
Total number of entries for port 2 radio 1: 5
Channel Neighbor BSS/MAC RSSI
------- ----------------- ----
1 00:0b:85:06:e3:60 -46
1 00:0b:0e:00:0a:80 -78
1 00:0b:0e:00:d2:c0 -74
1 00:0b:85:06:dd:00 -50
1 00:0b:0e:00:05:c1 -72

Table 64 describes the fields in this display.

**Table 64  Output for display auto-tune neighbors**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>Channel on which the BSSID is detected.</td>
</tr>
<tr>
<td>Neighbor BSS/MAC</td>
<td>BSSID detected by the radio.</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received signal strength indication (RSSI), in decibels referred to 1 milliwatt (dBm). A higher value indicates a stronger signal.</td>
</tr>
</tbody>
</table>

See Also

- **display auto-tune attributes** on page 386
- **display radio-profile** on page 398
- **set ap radio auto-tune max-power** on page 432
- **set ap radio auto-tune max- retransmissions** on page 433
- **set radio-profile auto-tune channel-config** on page 450
- **set radio-profile auto-tune channel-holddown** on page 451
- **set radio-profile auto-tune channel-interval** on page 452
- **set radio-profile auto-tune power-config** on page 454
- **set radio-profile auto-tune power-interval** on page 455
display ap boot-configuration

Displays information about the static IP address configuration (if any) on a
Distributed MAP.

**Syntax** — display ap boot-configuration *ap-number*

- *ap-number* — Index value that identifies the MAP on the WX.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2. Version 6.0 removed the *dap*
option, and added the following fields.

- Field Mesh
- Field Mesh SSID
- Field Mesh PSK

**Examples** — The following command displays static IP configuration
information for Distributed MAP 1:

```
WX# display ap boot-configuration 1
Static Boot Configuration
AP: 7
IP Address: Disabled
VLAN Tag: Disabled
Switch: Disabled
Mesh: Disabled
IP Address:
Netmask:
Gateway:
VLAN Tag:
Switch IP:
Switch Name:
Mesh SSID:
Mesh PSK:
```

Table 65 describes the fields in this display.
**Table 65** Output for display ap boot-configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Distributed MAP number.</td>
</tr>
<tr>
<td>IP address</td>
<td>Whether static IP address assignment is enabled for this Distributed MAP.</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>Whether the Distributed MAP is configured to use a VLAN tag.</td>
</tr>
<tr>
<td>Switch</td>
<td>Whether the Distributed MAP is configured to use a manually specified WX switch as its boot device.</td>
</tr>
<tr>
<td>Mesh</td>
<td>Whether WLAN mesh services are enabled for this MAP.</td>
</tr>
<tr>
<td>IP address</td>
<td>The static IP address assigned to this Distributed MAP.</td>
</tr>
<tr>
<td>Netmask</td>
<td>The subnet mask assigned to this Distributed MAP.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The IP address of the default gateway assigned to this Distributed MAP.</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>The VLAN tag that the Distributed MAP is configured to use (if any).</td>
</tr>
<tr>
<td>Switch IP</td>
<td>The IP address of the WX switch that this Distributed MAP is configured to use as its boot device (if any).</td>
</tr>
<tr>
<td>Switch Name</td>
<td>The name of the WX switch that this Distributed MAP is configured to use as its boot device (if any).</td>
</tr>
<tr>
<td>DNS IP</td>
<td>The IP address of the DNS server that the Distributed MAP uses to resolve the name of the WX switch used as its boot device.</td>
</tr>
<tr>
<td>Mesh SSID</td>
<td>The WLAN mesh services SSID this MAP is configured to use (if any)</td>
</tr>
<tr>
<td>Mesh PSK</td>
<td>The preshared key (PSK) the MAP uses for authentication with a Mesh Portal AP (if any).</td>
</tr>
</tbody>
</table>

**display ap connection**

Displays the system IP address of the WX switch that booted a Distributed MAP.

**Syntax** — `display ap connection [ap-number | serial-id serial-ID]`

- `ap-number` — Index value that identifies the MAP on the WX.
- `serial-id serial-ID` — MAP access point serial ID.

**Defaults** — None.

**Access** — Enabled.
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

History — Introduced in MSS Version 3.0. Version 6.0 removed the dap option.

Usage — The serial-id parameter displays the active connection for the specified Distributed MAP even if that MAP is not configured on this WX switch. If you instead use the command with the dap-num parameter or without a parameter, connection information is displayed only for Distributed MAPs that are configured on this WX switch.

This command provides information only if the Distributed MAP is configured on the switch where you use the command. The switch does not need to be the one that booted the MAP, but it must have the MAP in its configuration. Also, the switch that booted the MAP must be in the same Mobility Domain as the switch where you use the command.

If a Distributed MAP is configured on this WX switch (or another WX switch in the same Mobility Domain) but does not have an active connection, the command does not display information for the MAP. To show connection information for Distributed MAPs, use the display ap global command on one of the switches where the MAPs are configured.

Examples — The following command displays information for all Distributed MAPs configured on this WX switch that have active connections:

```
WX1200# display ap connection
Total number of entries: 2
    AP Serial Id   AP IP Address WX IP Address
--- ----------- --------------- ---------------
    2 M9DE48B012F00 10.10.2.27     10.3.8.111
    4 M9DE48B123400 10.10.3.34     10.3.8.111
```

The following command displays connection information specifically for a Distributed MAP with serial ID M9DE48B6EAD00:

```
WX1200# display ap connection serial-id M9DE48B6EAD00
Total number of entries: 1
    DAP Serial Id   DAP IP Address WX IP Address
--- ----------- --------------- ---------------
     9 M9DE48B6EAD00 10.10.4.88     10.9.9.11
```

Table 66 describes the fields in this display.
display ap global

Displays connection information for Distributed MAPs configured on a WX.

**Syntax** — `display ap global [ap-number | serial-id serial-ID]`

- `ap-number` — Index value that identifies the MAP on the WX.
- `serial-id serial-ID` — MAP access point serial ID.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 6.0 removed the `dap` option.

**Usage** — Connections are shown only for the Distributed MAPs that are configured on the WX switch from which you enter the command, and only for the Mobility Domain the switch is in.

To show information only for Distributed MAPs that have active connections, use the `display ap connection` command.

---

**Table 66** Output of `display ap connection`

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>ID assigned to the Distributed MAP.</td>
</tr>
<tr>
<td></td>
<td>If the connection is configured on another WX switch, this field contains a hyphen (<code>-</code>).</td>
</tr>
<tr>
<td>Serial Id</td>
<td>Serial ID of the Distributed MAP.</td>
</tr>
<tr>
<td>AP IP Address</td>
<td>IP address assigned by DHCP to the Distributed MAP.</td>
</tr>
<tr>
<td>WX IP Address</td>
<td>System IP address of the WX switch on which the MAP has an active connection. This is the switch that the MAP used for booting and configuration and is using for data transfer.</td>
</tr>
</tbody>
</table>

**See Also**

- `display ap config` on page 364
- `display ap global` on page 393
- `display ap unconfigured` on page 395
Examples — The following command displays configuration information for all the Distributed MAPs configured on a WX switch:

```
WX4400# display ap global
Total number of entries: 8
  AP Serial Id   WX IP Address   Bias
    ------------ --------------- ----
    1 M9DE48B012F00 10.3.8.111      HIGH
   - M9DE48B012F00 10.4.3.2        LOW
  2 M9DE48B123400 10.3.8.111      LOW
   - M9DE48B123400 10.4.3.2        HIGH
 17 M9DE48B123600 10.3.8.111      HIGH
  - M9DE48B123600 10.4.3.2        LOW
 18 M9DE48B123700 10.3.8.111      LOW
   - M9DE48B123700 10.4.3.2        HIGH
```

Table 67 describes the fields in this display.

Table 67 Output for display ap global

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP ID</td>
<td>ID assigned to the Distributed MAP.</td>
</tr>
<tr>
<td>Serial Id</td>
<td>Serial ID of the Distributed MAP.</td>
</tr>
<tr>
<td>WX IP Address</td>
<td>System IP address of the WX switch on which the Distributed MAP is configured.</td>
</tr>
<tr>
<td>Bias</td>
<td>Bias of the WX switch for the MAP:</td>
</tr>
<tr>
<td></td>
<td>• High</td>
</tr>
<tr>
<td></td>
<td>• Low</td>
</tr>
</tbody>
</table>

See Also

- `display ap config` on page 364
- `display ap connection` on page 391
- `display ap unconfigured` on page 395
- `set ap` on page 135
- `set ap bias` on page 415
**display ap unconfigured**

Displays Distributed MAPs that are physically connected to the network but that are not configured on any WX switches.

**Syntax** — `display ap unconfigured`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 6.0 removed the `dap` option.

**Usage** — This command also displays a MAP that is directly connected to a WX switch, if the WX port to which the MAP is connected is configured as a network port instead of a MAP access port, and if the network port is a member of a VLAN.

If a Distributed MAP is configured on a WX switch in another Mobility Domain, the MAP can appear in the output until the MAP is able to establish a connection with a WX switch in its Mobility Domain. After the MAP establishes a connection, the entry for the MAP ages out and no longer appears in the command's output.

Entries in the command output's table age out after two minutes.

**Examples** — The following command displays information for two Distributed MAPs that are not configured:

```plaintext
WX1200# display ap unconfigured
Total number of entries: 2
Serial Id   Model  IP Address      Port Vlan
------------- ------ --------------- ---- --------
M9DE48B012F00 AP2750 10.3.8.54       5    default
M9DE48B123400 AP2750 10.3.8.57       6  vlan-eng
```

Table 68 describes the fields in this display.

**Table 68**  Output for display ap unconfigured

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Id</td>
<td>Serial ID of the MAP.</td>
</tr>
<tr>
<td>Model</td>
<td>MAP model number.</td>
</tr>
</tbody>
</table>
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

See Also
- display ap connection on page 391
- display ap global on page 393

display load-balancing group

Displays an RF load balancing group’s member radios and current load for each radio.

Syntax — display load-balancing group {group-name | all} | {ap ap-number radio {1 | 2}}

- group-name — Name of an RF load-balancing group configured on the WX.
- all — Displays information for every load-balancing group that has a radio on this WX as a member.
- ap-name — Index value that identifies the MAP on the WX.
- radio {1 | 2} — Displays status information for a radio on an MAP. This option displays information about radios in the same group as the specified radio.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0. Version 6.0 removed the dap option.

Usage — Use this command to display information about the RF load-balancing groups configured on the WX and the individual MAP radios in the load-balancing groups.
**Examples** — The following command displays information about the MAP radios that are in the same group as radio 1 on MAP 3:

Rados in the same load-balancing group as: ap3/radio1

<table>
<thead>
<tr>
<th>IP address</th>
<th>AP</th>
<th>Radio</th>
<th>Overlap</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.28.200</td>
<td>3</td>
<td>1</td>
<td>100/100</td>
</tr>
</tbody>
</table>

The following command displays information about RF load balancing group `blue`:

Load-balancing group: blue

<table>
<thead>
<tr>
<th>IP address</th>
<th>AP</th>
<th>Radio</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.28.200</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 57 describes the fields in displayed by the `display load-balancing group` command.

**Table 69 Output for display load-balancing group**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IP address of the MAP in the load-balancing group.</td>
</tr>
<tr>
<td>AP</td>
<td>MAP number</td>
</tr>
<tr>
<td>Radio</td>
<td>Radio number</td>
</tr>
<tr>
<td>Overlap</td>
<td>The amount of overlapping coverage area the specified MAP radio has with the MAP radio in the list. An overlap of 100/100 indicates that the MAP radios have exactly the same coverage area.</td>
</tr>
<tr>
<td>Clients</td>
<td>The current client load on the MAP radio.</td>
</tr>
</tbody>
</table>

**See also**

- *set load-balancing strictness* on page 447
- *set ap radio load balancing* on page 437
- *set ap local-switching mode* on page 427
display radio-profile

Displays radio profile information.

**Syntax** — `display radio-profile {name | ?}

- `name` — Displays information about the named radio profile.
- `?` — Displays a list of radio profiles.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Name of the backoff timer field changed from Client Backoff Timer to Power Backoff Timer and new fields added in MSS Version 4.0:

- Countermeasures
- Active-Scan
- WMM enabled

Version 4.2 has the following changes:

- WMM enabled field renamed to QoS Mode.
- Long Retry Limit and Short Retry Limit fields moved to `display service-profile` output. (These options are now configurable on a service-profile basis instead of a radio-profile basis.)
- Allow 802.11g clients only field removed. (This option is now configured using the `set service-profile transmit-rates` command.)

**Usage** — MSS contains a `default` radio profile. 3Com recommends that you do not change this profile but instead keep the profile for reference.

**Examples** — The following command shows radio profile information for the `default` radio profile:

```
WX4400# display radio-profile default
Beacon Interval: 100   DTIM Interval: 1
Max Tx Lifetime: 2000  Max Rx Lifetime: 2000
RTS Threshold: 2346   Frag Threshold: 2346
Long Preamble: no     Tune Channel: yes
Tune Power: no        Tune Channel Interval: 3600
Tune Power Interval: 600  Channel Holddown: 300
Power Backoff Timer: 10  Countermeasures: none
Active-Scan: yes      QoS Mode: wmm
```
Table 70 describes the fields in this display.

**Table 70  Output for display radio-profile**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beacon Interval</td>
<td>Rate (in milliseconds) at which each MAP radio in the profile advertises the beaconed SSID.</td>
</tr>
<tr>
<td>DTIM Interval</td>
<td>Number of times after every beacon that each MAP radio in the radio profile sends a delivery traffic indication map (DTIM).</td>
</tr>
<tr>
<td>Max Tx Lifetime</td>
<td>Number of milliseconds that a frame received by a radio in the radio profile can remain in buffer memory.</td>
</tr>
<tr>
<td>Max Rx Lifetime</td>
<td>Number of milliseconds that a frame scheduled to be transmitted by a radio in the radio profile can remain in buffer memory.</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>Minimum length (in bytes) a frame can be for a radio in the radio profile to use the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.</td>
</tr>
<tr>
<td>Frag Threshold</td>
<td>Maximum length (in bytes) a frame is allowed to be without being fragmented into multiple frames before transmission by a radio in the radio profile.</td>
</tr>
</tbody>
</table>
| Long Preamble    | Indicates whether an 802.11b radio that uses this radio profile advertises support for frames with long preambles only:  
  - YES — Advertises support for long preambles only.  
  - NO — Advertises support for long and short preambles. |
| Tune Channel     | Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning channels. |
| Tune Power       | Indicates whether RF Auto-Tuning is enabled for dynamically setting and tuning power levels. |
| Tune Channel Interval | Interval, in seconds, at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed. |
| Tune Power Interval | Interval, in seconds, at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed. |
Table 70  Output for display radio-profile (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Holddown</td>
<td>Minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel.</td>
</tr>
<tr>
<td>Countermeasures</td>
<td>Indicates whether countermeasures are enabled.</td>
</tr>
<tr>
<td>Active-Scan</td>
<td>Indicates whether the active-scan mode of RF detection is enabled.</td>
</tr>
<tr>
<td>QoS Mode</td>
<td>Indicates the Quality-of-Service setting for MAP radio forwarding queues:</td>
</tr>
<tr>
<td></td>
<td>1. wmm—MAP forwarding queues provide standard priority handling for WMM devices.</td>
</tr>
<tr>
<td></td>
<td>2.svp—MAP forwarding queues are optimized for Spectralink Voice Priority (SVP).</td>
</tr>
<tr>
<td></td>
<td>For information about the QoS modes, see the “Configuring Quality of Service” chapter in the Wireless LAN Switch and Controller Configuration Guide.</td>
</tr>
<tr>
<td>Service profiles</td>
<td>Service profiles mapped to this radio profile. Each service profile contains an SSID and encryption information for that SSID.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When you upgrade from 2.x, MSS creates a default-dot1x service profile for encrypted SSIDs and a default-clear service profile for unencrypted SSIDs. These default service profiles contain the default encryption settings for crypto SSIDs and clear SSIDs, respectively.</td>
</tr>
</tbody>
</table>

See Also

- set radio-profile active-scan on page 448
- set radio-profile auto-tune channel-config on page 450
- set radio-profile auto-tune channel-holddown on page 451
- set radio-profile auto-tune channel-interval on page 452
- set radio-profile auto-tune power-config on page 454
- set radio-profile auto-tune power-interval on page 455
- set radio-profile beacon-interval on page 457
- set radio-profile countermeasures on page 458
- set radio-profile dtim-interval on page 460
- set radio-profile frag-threshold on page 461
- set radio-profile max-rx-lifetime on page 462
display service-profile

Displays service profile information.

**Syntax** — `display service-profile {name | ?}

- `name` — Displays information about the named service profile.
- `?` — Displays a list of service profiles.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. New fields added to indicate the configured SSID default attributes in the service profile. Version 4.2 added the following fields:

- Proxy ARP
- DHCP restrict
- No broadcast
- Short retry limit (moved from `display radio-profile` output)
- Long retry limit (moved from `display radio-profile` output)
- Sygate On-Demand (SODA)
- Enforce SODA checks:
- SODA remediation ACL
- Custom success web-page
- Custom failure web-page
- Custom logout web-page
- Custom agent-directory
- Static COS
- COS
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

- CAC mode
- CAC sessions
- User idle timeout
- Idle client probing
- Web Portal Session Timeout
- Transmit rates for 11a / 11b / 11g:
  - beacon rate
  - multicast rate
  - mandatory rate
  - standard rates
  - disabled rates

Version 6.0 removed the dap option, and added these new fields:

- Client DSCP
- Mesh enabled
- Bridging enabled
- Load Balance Exempt
- Web Portal Logout
- Custom Web Portal Logout URL
Examples — The following command displays information for service profile spl:

WX1200# **display service-profile spl**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssid-name:</td>
<td>corp2</td>
</tr>
<tr>
<td>ssid-type:</td>
<td>crypto</td>
</tr>
<tr>
<td>Beacon:</td>
<td>yes</td>
</tr>
<tr>
<td>DHCP restrict:</td>
<td>no</td>
</tr>
<tr>
<td>Short retry limit:</td>
<td>5</td>
</tr>
<tr>
<td>Auth fallback:</td>
<td>none</td>
</tr>
<tr>
<td>Enforce SODA checks:</td>
<td>yes</td>
</tr>
<tr>
<td>Custom success web-page:</td>
<td></td>
</tr>
<tr>
<td>Custom logout web-page:</td>
<td></td>
</tr>
<tr>
<td>Static COS:</td>
<td>no</td>
</tr>
<tr>
<td>CAC mode:</td>
<td>none</td>
</tr>
<tr>
<td>User idle timeout:</td>
<td>180</td>
</tr>
<tr>
<td>Web Portal Session Timeout:</td>
<td>5</td>
</tr>
<tr>
<td>WEP Key 1 value:</td>
<td>&lt;none&gt;</td>
</tr>
<tr>
<td>WEP Key 2 value:</td>
<td>&lt;none&gt;</td>
</tr>
<tr>
<td>WEP Key 3 value:</td>
<td>&lt;none&gt;</td>
</tr>
<tr>
<td>WEP Key 4 value:</td>
<td>&lt;none&gt;</td>
</tr>
<tr>
<td>WEP Unicast Index:</td>
<td>1</td>
</tr>
<tr>
<td>WEP Multicast Index:</td>
<td>1</td>
</tr>
<tr>
<td>Shared Key Auth:</td>
<td>NO</td>
</tr>
<tr>
<td>WPA enabled:</td>
<td></td>
</tr>
<tr>
<td>ciphers:</td>
<td></td>
</tr>
<tr>
<td>authentication:</td>
<td>802.1X</td>
</tr>
<tr>
<td>TKIP countermeasures time:</td>
<td>60000ms</td>
</tr>
<tr>
<td>vlan-name = orange</td>
<td></td>
</tr>
<tr>
<td>session-timeout = 300</td>
<td></td>
</tr>
<tr>
<td>service-type = 2</td>
<td></td>
</tr>
<tr>
<td>11a beacon rate:</td>
<td>6.0</td>
</tr>
<tr>
<td>11a mandatory rate:</td>
<td>6.0,12.0,24.0</td>
</tr>
<tr>
<td>11a standard rates:</td>
<td>9.0,18.0,36.0,48.0,54.0</td>
</tr>
<tr>
<td>11b beacon rate:</td>
<td>2.0</td>
</tr>
<tr>
<td>11b mandatory rate:</td>
<td>1.0,2.0</td>
</tr>
<tr>
<td>11b standard rates:</td>
<td>5.5,11.0</td>
</tr>
<tr>
<td>11g beacon rate:</td>
<td>2.0</td>
</tr>
<tr>
<td>11g mandatory rate:</td>
<td>1.0,2.0,5.5,11.0</td>
</tr>
<tr>
<td>11g standard rates:</td>
<td>6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0</td>
</tr>
</tbody>
</table>

Table 71 describes the fields in this display.
**Table 71** Output for display service-profile

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssid-name</td>
<td>Service set identifier (SSID) managed by this service profile.</td>
</tr>
</tbody>
</table>
| ssid-type     | SSID type:  
|               | - **crypto** — Wireless traffic for the SSID is encrypted.                                                                                   |
|               | - **clear** — Wireless traffic for the SSID is unencrypted.                                                                                   |
| beacon        | Indicates whether the radio sends beacons, to advertise the SSID:  
|               | - no  
|               | - yes                                                                                                                                    |
| Proxy ARP     | Indicates whether proxy ARP is enabled. When this feature is enabled, MSS answers ARP requests on behalf of wireless clients.                |
| DHCP restrict | Indicates whether DHCP Restrict is enabled. When this feature is enabled, MSS allows only DHCP traffic for a new client until the client has successfully completed authentication and authorization. |
| No broadcast  | Indicates whether broadcast restriction is enabled. When this feature is enabled, MSS sends ARP requests and DHCP Offers and Acks as unicasts to their target clients instead of forwarding them as broadcasts. |
| Short retry limit | Number of times a radio serving the service-profile’s SSID can send a short unicast frame without receiving an acknowledgment.              |
| Long retry limit | Number of times a radio serving the service-profile’s SSID can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is equal to or longer than the RTS threshold. |
| auth-fallthru | Secondary (fallthru) encryption type when a user tries to authenticate but the WX switch managing the radio does not have an authentication rule with a userglob that matches the username:  
|               | - **last-resort** — Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password. |
|               | - **none**—Denies authentication and prohibits the user from accessing the SSID.                                                              |
|               | - **web-auth** — Redirects the user to a web page for login to the SSID.                                                                     |
### Table 71  Output for display service-profile (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sygate On-Demand (SODA)</td>
<td>Whether SODA functionality is enabled for the service profile. When SODA functionality is enabled, connecting clients download SODA agent files, which perform security checks on the client.</td>
</tr>
<tr>
<td>Enforce SODA checks</td>
<td>Whether a client is allowed access to the network after it has downloaded and run the SODA agent security checks. When SODA functionality is enabled, and the WX switch is configured to enforce SODA checks, then a connecting client must download the SODA agent files and pass the checks in order to gain access to the network.</td>
</tr>
<tr>
<td>SODA remediation ACL</td>
<td>The name of the ACL to be applied to the client if it fails the SODA agent checks. If no remediation ACL is specified, then a client is disconnected from the network if it fails the SODA agent checks.</td>
</tr>
<tr>
<td>Custom success web-page</td>
<td>The name of the user-specified page that the client loads upon successful completion of the SODA agent checks. If no page is specified, then the success page is generated dynamically.</td>
</tr>
<tr>
<td>Custom failure web-page</td>
<td>The name of the user-specified page that the client loads if it fails SODA agent checks. If no page is specified, then the failure page is generated dynamically.</td>
</tr>
<tr>
<td>Custom logout web-page</td>
<td>The name of the user-specified page that the client loads upon logging out of the network, either by closing the SODA virtual desktop, or by requesting the page. If no page is specified, then the client is disconnected without loading a logout page.</td>
</tr>
<tr>
<td>Custom agent-directory</td>
<td>The name of the directory for SODA agent files on the WX switch, if different from the default. By default, SODA agent files are stored in a directory with the same name as the service profile.</td>
</tr>
<tr>
<td>Static COS</td>
<td>Indicates whether static CoS assignment is enabled. When this feature is enabled, MAPs assign the CoS value in the COS field to all user traffic forwarded by the MAP.</td>
</tr>
<tr>
<td>COS</td>
<td>CoS value assigned by the MAP to all user traffic, if static CoS is enabled. (If static CoS is disabled, WMM or ACLs are used to assign CoS.)</td>
</tr>
<tr>
<td>Client DSCP</td>
<td>Whether packets are classified based on client DSCP level instead of 802.11 priority.</td>
</tr>
</tbody>
</table>
### Table 71  Output for display service-profile (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAC mode</td>
<td>Call Admission Control mode:</td>
</tr>
<tr>
<td></td>
<td>- none—CAC is disabled.</td>
</tr>
<tr>
<td></td>
<td>- session—CAC is based on the number of active user sessions. If a MAP radio reaches the maximum</td>
</tr>
<tr>
<td></td>
<td>number of active user sessions specified in the CAC session field, the MAP radio rejects</td>
</tr>
<tr>
<td></td>
<td>new connection attempts.</td>
</tr>
<tr>
<td>CAC sessions</td>
<td>Maximum number of user sessions that can be active on a MAP radio at one time, if the CAC mode</td>
</tr>
<tr>
<td></td>
<td>is session. (If the CAC mode is none, this value is not used.)</td>
</tr>
<tr>
<td>User idle timeout</td>
<td>Indicates how many seconds a user session can remain idle (indicated by no user traffic and no</td>
</tr>
<tr>
<td></td>
<td>reply to client keepalive probes) before the session is changed to the Disassociated state.</td>
</tr>
<tr>
<td>Idle client probing</td>
<td>Indicates whether client keepalive probes are enabled.</td>
</tr>
<tr>
<td>Web Portal Session Timeout</td>
<td>When a Web Portal WebAAA session is placed in the Deassociated state, how many seconds the</td>
</tr>
<tr>
<td></td>
<td>session can remain in that state before being terminated automatically.</td>
</tr>
<tr>
<td>Mesh enabled</td>
<td>Whether WLAN mesh services are enabled for the service profile.</td>
</tr>
<tr>
<td>Bridging enabled</td>
<td>Whether wireless bridging is enabled for this service profile.</td>
</tr>
<tr>
<td>Load Balance Exempt</td>
<td>Whether the MAP radios managed by this service profile are exempted (do not participate in) RF</td>
</tr>
<tr>
<td></td>
<td>load balancing.</td>
</tr>
<tr>
<td>Web Portal Logout</td>
<td>Whether the Web Portal WebAAA logout functionality has been enabled.</td>
</tr>
<tr>
<td>Custom Web Portal Logout URL</td>
<td>If configured, the URL that Web Portal WebAAA users can access in order to terminate their</td>
</tr>
<tr>
<td></td>
<td>sessions.</td>
</tr>
<tr>
<td>WEP Key 1 value</td>
<td>State of static WEP key number 1. Radios can use this key to encrypt traffic with static Wired-</td>
</tr>
<tr>
<td></td>
<td>Equivalent Privacy (WEP):</td>
</tr>
<tr>
<td></td>
<td>- none — The key is not configured.</td>
</tr>
<tr>
<td></td>
<td>- preset — The key is configured.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The WEP parameters apply to traffic only on the encrypted SSID.</td>
</tr>
<tr>
<td>WEP Key 2 value</td>
<td>State of static WEP key number 2:</td>
</tr>
<tr>
<td></td>
<td>- none — The key is not configured.</td>
</tr>
<tr>
<td></td>
<td>- preset — The key is configured.</td>
</tr>
</tbody>
</table>
**Table 71  Output for display service-profile (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| WEP Key 3 value        | State of static WEP key number 3:  
  - **none** — The key is not configured.  
  - **preset** — The key is configured. |
| WEP Key 4 value        | State of static WEP key number 4:  
  - **none** — The key is not configured.  
  - **preset** — The key is configured. |
| WEP Unicast Index      | Index of the static WEP key used to encrypt unicast traffic on an encrypted SSID.                                                             |
| WEP Multicast Index    | Index of the static WEP key used to encrypt multicast traffic on an encrypted SSID.                                                           |
| Shared Key Auth        | Indicates whether shared-key authentication is enabled.                                                                                     |
| WPA enabled or RSN enable | Indicates that the Wi-Fi Protected Access (WPA) information element (IE) is enabled. Additional fields display the settings of other WPA parameters:  
  - **ciphers** — Lists the WPA cipher suites advertised by radios in the radio profile mapped to this service profile.  
  - **authentication** — Lists the authentication methods supported for WPA or RSN clients:  
    - **802.1X** — dynamic authentication  
    - **PSK** — preshared key authentication  
  - **TKIP countermeasures time** — Indicates the amount of time (in ms) MSS enforces countermeasures following a second message integrity code (MIC) failure within a 60-second period.  
  **Note:** These fields are displayed only when the WPA IE or RSN IE is enabled. |
| vlan-name, session-timeout, service-type | These are examples of authorization attributes that are applied by default to a user accessing the SSID managed by this service profile (in addition to any attributes assigned to the user by a RADIUS server or the local database).  
Attributes are listed here only if they have been configured as default attribute settings for the service profile.  
See Table 45 on page 310 for a list of authorization attributes and values that can be assigned to network users. |
Table 71  Output for display service-profile (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11a / 11b / 11g transmit rate fields</td>
<td>Data transmission rate settings for each radio type:</td>
</tr>
<tr>
<td></td>
<td>● beacon rate—Data rate of beacon frames sent by MAP radios.</td>
</tr>
<tr>
<td></td>
<td>● multicast rate—Data rate of multicast frames sent by MAP radios. If the rate is auto, the MAP sets the multicast rate to the highest rate that can reach all clients connected to the radio.</td>
</tr>
<tr>
<td></td>
<td>● mandatory rates—Set of data transmission rates that clients are required to support in order to associate with an SSID on a MAP radio. A client must support at least one of the mandatory rates.</td>
</tr>
<tr>
<td></td>
<td>● standard rates—The set of valid rates that are neither mandatory nor disabled. These rates are supported for data transmission from the MAP radios.</td>
</tr>
<tr>
<td></td>
<td>● disabled rates—Data transmission rates that MAP radios will not use to transmit data. (The radios will still accept frames from clients at disabled data rates.)</td>
</tr>
</tbody>
</table>

See Also

- set service-profile auth-dot1x on page 481
- set service-profile auth-fallthru on page 482
- set service-profile auth-psk on page 483
- set service-profile auth-psk on page 483
- set service-profile beacon on page 484
- set service-profile cac-mode on page 486
- set service-profile cac-session on page 487
- set service-profile cipher-ccmp on page 488
- set service-profile cipher-tkip on page 489
- set service-profile cipher-wep104 on page 490
- set service-profile cipher-wep40 on page 491
- set service-profile cos on page 492
- set service-profile dhcp-restrict on page 493
- set service-profile idle-client-probing on page 494
- set service-profile long-retry-count on page 497
- set service-profile no-broadcast on page 499
- set service-profile proxy-arp on page 500
- set service-profile psk-phrase on page 501
- set service-profile psk-raw on page 502
- set service-profile rsn-ie on page 503
- set service-profile shared-key-auth on page 504
- set service-profile short-retry-count on page 504
- set service-profile soda mode on page 510
- set service-profile ssid-name on page 513
- set service-profile ssid-type on page 514
- set service-profile static-cos on page 515
- set service-profile tkip-mc-time on page 514
- set service-profile transmit-rates on page 516
- set service-profile user-idle-timeout on page 519
- set service-profile web-portal-form on page 521
- set service-profile web-portal-session-timeout on page 525
- set service-profile wep active-multicast-index on page 526
- set service-profile wep active-unicast-index on page 527
- set service-profile wep key-index on page 528
- set service-profile wpa-ie on page 529
reset ap

Restarts a MAP access point.

**Syntax** — `reset ap ap-number`
- `ap ap-number` — Index value that identifies the MAP on the WX.
- `dap dap-num` — Number of a Distributed MAP to reset.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 6.0 removed the `dap` option.

**Usage** — When you enter this command, the MAP drops all sessions and reboots.

⚠️ **CAUTION:** Restarting a MAP can cause data loss for users who are currently associated with the MAP.

**Examples** — The following command resets MAP 7:

```
WX1200# reset ap 7
This will reset specified AP devices.
Would you like to continue? (y/n) y
success: rebooting ap attached to port 7
```

set ap auto

Creates a profile for automatic configuration of MAPs.

**Syntax** — `set ap auto`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 4.0. Version 6.0 removed the `dap` option.

**Usage** — Table 72 lists the configurable profile parameters and their defaults. The only parameter that requires configuration is the profile mode. The profile is disabled by default. To use the profile to configure Distributed MAPs, you must enable the profile using the `set ap auto mode enable` command.
The profile uses the default radio profile by default. You can change the profile using the set ap auto radio radio-profile command. You can use set ap auto commands to change settings for the parameters listed in Table 72. (The commands are listed in the “See Also” section.)

Table 72  Configurable Profile Parameters for Distributed MAPs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAP Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>bias</td>
<td>high</td>
</tr>
<tr>
<td>blink</td>
<td>disable</td>
</tr>
<tr>
<td>(Not shown in display ap config output)</td>
<td></td>
</tr>
<tr>
<td>force-image-download</td>
<td>disable (NO)</td>
</tr>
<tr>
<td>group (load balancing group)</td>
<td>none</td>
</tr>
<tr>
<td>mode</td>
<td>disabled</td>
</tr>
<tr>
<td>persistent</td>
<td>none</td>
</tr>
<tr>
<td>upgrade-firmware (boot-download-enabled)</td>
<td>enable (YES)</td>
</tr>
<tr>
<td><strong>Radio Parameters</strong></td>
<td></td>
</tr>
<tr>
<td>radio num auto-tune max-power</td>
<td>default</td>
</tr>
<tr>
<td>radio num mode</td>
<td>enabled</td>
</tr>
<tr>
<td>radio num radio-profile</td>
<td>default</td>
</tr>
<tr>
<td>radiotype</td>
<td>11g</td>
</tr>
<tr>
<td>(or 11b for country codes where 802.11g is not allowed)</td>
<td></td>
</tr>
</tbody>
</table>

Examples — The following command creates a profile for automatic Distributed MAP configuration:

WX1200# set ap auto
success: change accepted.

See Also
- set ap auto mode on page 414
- set ap auto persistent on page 412
- set ap auto radiotype on page 413
- set ap bias on page 415
set ap blink on page 416
set ap group on page 427
set ap radio auto-tune max-power on page 432
set ap radio auto-tune max-retransmissions on page 433
set ap radio link-calibration on page 436
set ap radio mode on page 439
set ap radio radio-profile on page 440
set ap upgrade-firmware on page 444

set ap auto persistent

Converts a temporary MAP configuration created by the MAP configuration profile into a persistent MAP configuration on the WX.

Syntax — set ap auto persistent [ap-number | all]

- **ap-number** — Index value that identifies the MAP on the WX.
- **all** — Converts the configurations of all Auto-APs being managed by the switch into permanent configurations.

Defaults — None.

Access — Enabled.

History — Introduced in MSS 4.0. Version 6.0 removed the dap option.

Usage — To display the Distributed MAP numbers assigned to Auto-MAPS, use the display ap status auto command.

Examples — The following command converts the configuration of Auto-AP 10 into a permanent configuration:

```shell
WX4400# set ap auto persistent 10
success: change accepted.
```

See Also

- set ap auto on page 410
- set ap auto mode on page 414
- set ap auto radiotype on page 413
**set ap auto radiotype**

Sets the radio type for single-MAP radios that use the MAP configuration profile.

**Syntax** — `set ap auto [radiotype {11a | 11b | 11g}]`

- `radiotype {11a | 11b | 11g}` — Radio type. (The 11a option applies only to single-radio models. The 802.11a radio in two-radio models is always 802.11a.):
  - 11a — 802.11a
  - 11b — 802.11b
  - 11g — 802.11g

**Defaults** — The default radio type for model AP2750 and for the 802.11b/g radios in other models is 802.11g in regulatory domains that support 802.11g, or 802.11b in regulatory domains that do not support 802.11g.

**Access** — Enabled.

**History** — Version 6.0 removed the dap option.

**Examples** — The following command sets the radio type to 802.11b:

```
WX4400# set ap auto radiotype 11b
success: change accepted.
```

**See Also**

- `set ap auto` on page 410
- `set ap auto mode` on page 414
- `set ap auto persistent` on page 412
**set ap auto mode**

Enables a WX profile for automatic Distributed MAP configuration.

**Syntax** — `set ap auto mode {enable | disable}`

- `enable` — Enables the MAP configuration profile.
- `disable` — Disables the MAP configuration profile.

**Defaults** — The MAP configuration profile is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS 4.0. Version 6.0 removed the `dap` option.

**Usage** — You must use the `set ap auto` command to create the profile before you can enable it.

**Examples** — The following command enables the profile for automatic Distributed MAP configuration:

```
WX4400# set ap auto mode enable
success: change accepted.
```

**See Also**

- `set ap auto` on page 410
- `set ap auto persistent` on page 412
- `set ap auto radiotype` on page 413
- `set ap bias` on page 415
- `set ap blink` on page 416
- `set ap group` on page 427
- `set ap radio auto-tune max-power` on page 432
- `set ap radio auto-tune max-retransmissions` on page 433
- `set ap radio link-calibration` on page 436
- `set ap radio mode` on page 439
- `set ap radio radio-profile` on page 440
- `set ap upgrade-firmware` on page 444
**set ap bias**

Changes the bias for a MAP. Bias is the priority of one WX over other WX switches for booting and configuring the MAP.

**Syntax** — `set ap ap-number auto bias {high | low}`

- **ap ap-number** — Index value that identifies the MAP on the WX.
- **ap auto** — Configures bias for the MAP configuration profile. (See `set ap auto` on page 410.)
- **high** — High bias.
- **low** — Low bias.

**Defaults** — The default bias is high.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Option **auto** added for configuration of the MAP configuration profile. Version 6.0 removed the **dap** option.

**Usage** — High bias is preferred over low bias. Bias applies only to WX switches indirectly attached to the MAP through an intermediate Layer 2 or Layer 3 network. A MAP always attempts to boot on MAP port 1 first, and if an WX is directly attached on MAP port 1, the MAP always boots from it.

If MAP port 1 is indirectly connected to WX switches through the network, the MAP boots from the WX with the high bias for the MAP. If the bias for all connections is the same, the MAP selects the WX that has the greatest capacity to add more active MAPs. For example, if a MAP is dual homed to two WX4400 wireless LAN switches, and one of the switches has 50 active MAPs while the other WX has 60 active MAPs, the new MAP selects the WX that has only 50 active MAPs.

If the boot request on MAP port 1 fails, the MAP attempts to boot over its port 2, using the same process described above.

MAP selection of a WX is *sticky*. After a MAP selects a WX to boot from, the MAP continues to use that WX for its active data link even if another switch configured with high bias for the MAP becomes available.
Examples — The following command changes the bias for a Distributed MAP to low:

WX4400# set dap 1 bias low
success: change accepted.

See Also
- display ap config on page 364

---

**set ap blink**

Enables or disables LED blink mode on a MAP to make it easy to identify. When blink mode is enabled on (MAP-xxx models, the health and radio LEDs alternately blink green and amber. By default, blink mode is disabled.

Syntax — set {ap ap-number auto blink {enable | disable}}
- ap ap-number — Index value that identifies the MAP on the WX.
- enable — Enables blink mode.
- disable — Disables blink mode.

Defaults — LED blink mode is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option auto added for configuration of the MAP configuration profile. Version 6.0 removed the dap option.

Usage — Changing the LED blink mode does not alter operation of the MAP access point. Only the behavior of the LEDs is affected.

Examples — The following command enables LED blink mode on the MAP access points connected to ports 3 and 4:

WX1200# set ap 3-4 blink enable
success: change accepted.
**set ap boot-configuration ip**

Specifies static IP address information for a Distributed MAP.

**Syntax** — `set ap ap-number boot-configuration ip ip-addr netmask mask-addr gateway gateway-addr [mode {enable | disable}]`

**Syntax** — `set dap dap-num boot-ip mode {enable | disable}`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `ip ip-addr` — The IP address to be assigned to the MAP, in dotted decimal notation (for example, 10.10.10.10).
- `netmask mask-addr` — The subnet mask, in dotted decimal notation (for example, 255.255.255.0).
- `gateway gateway-addr` — The IP address of the next-hop router, in dotted decimal notation.
- `mode {enable | disable}` — Enables or disables the static IP address for the MAP.

**Defaults** — By default MAPs use DHCP to obtain an IP address, rather than a manually assigned IP address.

**Access** — Enabled.

**History** — Introduced in MSS version 4.2. Version 6.0 removed the **dap** option.

**Usage** — Normally, Distributed MAPs use DHCP to obtain IP address information. In some installations, DHCP may not be available. In this case, you can assign static IP address information to the MAP, including the MAP IP address and netmask, and default gateway.

If the manually assigned IP information is incorrect, the MAP uses DHCP to obtain its IP address.

**Examples** — The following command configures MAP 1 to use IP address 172.16.0.42 with a 24-bit netmask, and use 172.16.0.20 as its default gateway:

```
WX4400# set ap 1 boot-configuration ip 172.16.0.42 netmask 255.255.255.0 gateway 172.16.0.20
success: change accepted.
```
See Also

- `clear ap boot-configuration` on page 358
- `display ap boot-configuration` on page 390
- `set ap boot-configuration vlan` on page 423

---

**set ap boot-configuration mesh mode**

Enables WLAN mesh services on the MAP.

**Syntax** — `set ap ap-number boot-configuration mesh mode [mode {enable | disable}]`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `mode {enable | disable}` — Enables or disables WLAN mesh services for the MAP.

**Defaults** — Disabled.

**Access** — Enabled.

**History** — Introduced in MSS version 6.0.

**Usage** — Use this command to enable WLAN mesh services for an Mesh AP. Prior to deploying the Mesh AP in its final untethered location, you must connect the MAP to an WX and enter this command to configure the MAP for mesh services.

**Examples** — The following command enables WLAN mesh services for MAP 7:

```
WX4400# set ap 7 boot-configuration mesh mode enable
success: change accepted.
```

See Also

- `display ap mesh-links` on page 377
- `set ap boot-configuration mesh ssid` on page 421
- `set service-profile mesh` on page 498
### set ap boot-configuration mesh psk-phrase

Specifies a preshared key (PSK) phrase that a Mesh AP uses for authentication to its Mesh Portal AP.

**Syntax** — `set ap ap-number boot-configuration mesh psk-phrase passphrase`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `passphrase` — An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — Use this command to configure the preshared key that a Mesh AP uses to authenticate to a Mesh Portal AP. You must connect the MAP to an WX switch and enter this command to configure the MAP for mesh services prior to deploying the Mesh AP in its final untethered location.

MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the WX configuration. Neither the binary number nor the passphrase itself is ever displayed in the configuration. To use PSK authentication, you must enable it and you also must enable the WPA IE.

**Examples** — The following command configures MAP 7 to use passphrase “1234567890123<>?+=&% The quick brown fox jumps over the lazy sl” when authenticating with a Mesh Portal AP

```
WX# set ap 7 boot-configuration mesh psk-phrase "1234567890123<>?+=&% success: change accepted.
```

**See Also**
- `display ap mesh-links` on page 377
- `set ap boot-configuration mesh ssid` on page 421
- `set service-profile mesh` on page 498
set ap boot-configuration mesh psk-raw

Configures a raw hexadecimal preshared key (PSK) to use for authenticating a Mesh AP to a Mesh Portal AP. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax — set ap ap-number boot-configuration mesh psk-raw hex

- ap ap-number — Index value that identifies the MAP on the WX.
- hex — A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Use this command to configure the preshared key that a Mesh AP uses to authenticate to a Mesh Portal AP. You must connect the MAP to an WX switch and enter this command to configure the MAP for mesh services prior to deploying the Mesh AP in its final untethered location.

MSS converts the hexadecimal into a 256-bit binary number for system use. MSS also stores the hexadecimal key in the WX configuration. The binary number is never displayed in the configuration. To use PSK authentication, you must enable it and you also must enable the WPA IE.

Examples — The following command configures MAP 7 to use a raw PSK to authenticate with a Mesh Portal AP:

WX# set ap 7 boot-configuration mesh psk-raw c25d3fe4483e867d1df96eeacdf8b02451fa0836162e758100f5f6b87965 e59d
success: change accepted.

See Also

- display ap mesh-links on page 377
- set ap boot-configuration mesh ssid on page 421
- set service-profile mesh on page 498
### set ap boot-configuration mesh ssid

Specifies the name of the SSID a Mesh AP attempts to associate with when it is booted.

**Syntax** — `set ap ap-number boot-configuration mesh ssid mesh-ssid`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `mesh-ssid` — Name of the mesh SSID (up to 32 characters).

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — You must connect the MAP to a WX switch and enter this command to specify the mesh SSID prior to deploying the Mesh AP in its final untethered location. When the MAP is booted its untethered location, and it determines that it has no Ethernet link to the network, it then associates with the specified `mesh-ssid`.

Note that when the `mesh-ssid` is specified, the regulatory domain of the WX and the power restrictions are copied to the MAP flash memory. This prevents the Mesh AP from operating outside of regulatory limits after it is booted and before it receives its complete configuration from the WX. Consequently, it is important that the regulatory and antenna information specified on the WX actually reflects the locale where the Mesh AP is to be deployed, in order to avoid regulatory violations.

**Examples** — The following command configures MAP 7 to attempt to associate with the SSID `wlan-mesh` when booted in an untethered location:

```bash
WX# set ap 7 boot-configuration mesh ssid wlan-mesh
success: change accepted.
```

- [display ap mesh-links](page 377)
- [set ap boot-configuration mesh mode](page 418)
- [set service-profile mesh](page 498)
set ap boot-configuration switch

Specifies the WX a Distributed MAP contacts and attempts to use as its boot device.

**Syntax** — `set ap ap-number boot-configuration switch`  

- `ap-number` — Index value that identifies the MAP on the WX.
- `switch-ip ip-addr` — The IP address of the WX switch the Distributed MAP should boot from.
- `name name dns ip-addr` — The fully qualified domain name of the WX the Distributed MAP should boot from. When both a name and a switch-ip are specified, the MAP uses the name.
- `dns ip-addr` — The IP address of the DNS server used to resolve the specified name of the WX switch.
- `mode {enable | disable}` — Enables or disables the MAP using the specified boot device.

**Defaults** — By default MAPs use the process described in “Default MAP Boot Process”, in the Wireless LAN Switch and Controller Configuration Guide to boot from a WX, instead of using a manually specified WX.

**Examples** — Enabled.

**History** — Introduced in MSS 4.2. Version 6.0 removed the `dap` option.

**Usage** — When you specify a boot WX for a distributed MAP to boot from, it boots using the process described in “MAP Boot Process Using Static IP Configuration”, in the Wireless LAN Switch and Controller Configuration Guide.

When a static IP address is specified for a Distributed MAP, there is no preconfigured DNS information or DNS name for the WX the Distributed MAP attempts to use as its boot device. If you configure a static IP address for a Distributed MAP, but do not specify a boot device, then the WX must be reachable via subnet broadcast.

**Examples** — The following command configures Distributed MAP 1 to use the WX with address 172.16.0.21 as its boot device.
WX1200# set ap 1 boot-configuration switch switch-ip 172.16.0.21 mode enable
success: change accepted.

The following command configures Distributed MAP 1 to use the WX with the name wxr2 as its boot device. The DNS server at 172.16.0.1 is used to resolve the name of the WX switch.

WX4400# set ap 1 boot-configuration switch name wxr2 dns 172.16.0.1 mode enable
success: change accepted.

See Also
- clear ap boot-configuration on page 358
- display ap boot-configuration on page 390
- set ap boot-configuration ip on page 417
- set ap boot-configuration vlan on page 423

set ap boot-configuration vlan

Specifies 802.1Q VLAN tagging information for a Distributed MAP.

Syntax — set ap ap-number boot-configuration vlan vlan-tag tag-value [mode {enable | disable}]

Syntax — set ap ap-number boot-configuration vlan mode {enable | disable}

- ap ap-number — Index value that identifies the MAP on the WX.
- vlan-tag tag-value — The VLAN tag value. You can specify a number from 1 – 4095.
- mode {enable | disable} — Enables or disables use of the specified VLAN tag on the Distributed MAP.

Defaults — None.

Examples — Enabled.

History — Introduced in MSS 4.2. Version 6.0 removed the dap option.
**Usage** — When this command is configured, all Ethernet frames emitted from the Distributed MAP are formatted with an 802.1Q tag with a specified VLAN number. Frames sent to the Distributed MAP that are not tagged with this value are ignored.

**Examples** — The following command configures Distributed MAP 1 to use VLAN tag 100:

```
WX4400# set ap 1 boot-configuration vlan vlan-tag 100 mode enable
success: change accepted.
```

**See Also**

- `clear ap boot-configuration` on page 358
- `display ap boot-configuration` on page 390
- `set ap boot-configuration ip` on page 417

### set ap contact

Specifies information about the contact information for the MAP.

**Syntax** — `set ap port-list contact string`

**Examples** — The following command specifies the contact person as Bob:

```
WX4400# set ap 7 contact 'Bob'
success: change accepted.
```

**See Also**

- `set ap location` on page 427
- `display ap config` on page 364

### set ap fingerprint

Verifies a MAP fingerprint on a WX. If MAP-WX security is required by a WX, a MAP can establish a management session with the switch only if you have verified the MAP identity by verifying its fingerprint on the switch.

**Syntax** — `set ap ap-number fingerprint fingerprint`

- `ap ap-num` — Index value that identifies the MAP on the WX.
- **fingerprint** — The 16-digit hexadecimal number of the fingerprint. Use a colon between each digit. Make sure the fingerprint you enter matches the fingerprint used by the MAP.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 4.0. Version 6.0 removed the dap option.

**Usage** — MAPs are configured with an encryption key pair at the factory. The fingerprint for the public key is displayed on a label on the back of the MAP, in the following format:

```
RSA
aaaa:aaaa:aaaa:aaaa:
aaaa:aaaa:aaaa:aaaa
```

If a MAP is already installed and operating, you can use the **display ap status** command to display the fingerprint. The **display ap config** command lists a MAP fingerprint only if the fingerprint has been verified in MSS. If the fingerprint has not been verified, the fingerprint information in the command output is blank.

**Examples** — The following example verifies the fingerprint for Distributed MAP 8:

```
WX4400# set ap 8 fingerprint
success: change accepted.
```

**See Also**

- **display ap config** on page 364
- **display ap status** on page 379
- **set ap security** on page 443
set ap force-image-download

Configures a MAP to download a software image from the WX instead of loading the image locally stored on the MAP.

**Syntax** — `set ap auto force-image-download {enable | disable}`

- **ap auto**—Configures forced image download for the MAP configuration profile.
- **force-image-download enable**—Enables forced image download.
- **force-image-download disable**—Disables forced image download.

**Defaults** — Forced image download is disabled by default.

**Access** — Enabled.

**History** — Version 5.0 Command introduced. Version 6.0 Option `dap` removed.

**Usage** — A change to the forced image download option takes place the next time the MAP is restarted.

Even when forced image download is disabled (the default), the MAP still checks with the WX to verify that the MAP has the latest image, and to verify that the WX is running MSS Version 5.0 or later.

The MAP loads a local image only if the WX is running MSS Version 5.0 or later and does not have a different MAP image than the one in the MAP local storage. If the WX is not running MSS Version 5.0 or later, or the WX has a different version of the MAP image than the current version on the MAP, the MAP loads an image from the WX.

**Examples** — The following command enables forced image download on Distributed MAP 69:

`WX1200# set ap 69 force-image-download enable`

success: change accepted.

**See Also**

- `display ap config` on page 364
### set ap group

Deprecated in MSS Version 6.0. To configure RF load balancing, see “set load-balancing mode” on page 446.

### set ap location

Specifies information about the physical location of a MAP.

**Syntax** — `set ap port-list location string`

**Examples** — The following command specifies the location of MAP 7 as the conference room:

```
WX4400# set ap 7 location 'the conference room'
success: change accepted.
```

**See Also**
- [set ap contact](#) on page 424
- [display ap config](#) on page 364

### set ap local-switching mode

Enables local switching for a specified MAP.

**Syntax** — `set ap ap-number local-switching mode {enable | disable}`

- `ap-number` — Index value that identifies the MAP on the WX.
- `mode {enable | disable}` — Enables or disables local switching for the MAP.

**Defaults** — Local switching is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — Local switching allows traffic for specified VLANs to be switched by the MAP itself, instead of being tunneled back to a WX. The VLANs for which local switching is performed are specified in a VLAN profile.

Local switching can be enabled on MSPs that are connected to the WX via an intermediate Layer 2 or Layer 3 network. Local switching is not supported for MAPs that are directly connected to an WX.
If local switching is enabled on an MAP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named `default` that is not tagged.

**Examples** — The following command enables local switching for MAP 7:

```
WX# set ap 7 local-switching mode enable
success: change accepted.
```

**See Also**
- `set ap local-switching vlan-profile` on page 428
- `set vlan profile` on page 175

---

**set ap local-switching vlan-profile**

Applies a specified VLAN profile to an MAP to use with local switching.

**Syntax** — `set ap ap-number local-switching vlan-profile profile name`

- `ap-number` — Index value that identifies the MAP on the WX.
- `profile-name` — The name of a VLAN profile configured on the WX.

**Defaults** — If local switching is enabled on an MAP, but no VLAN profile is configured, then a default VLAN profile is used. The default VLAN profile includes a single VLAN named `default` that is not tagged.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**History** — A VLAN profile consists of a list of VLANs and tags. When a VLAN profile is applied to an MAP, traffic for the VLANs specified in the VLAN profile is locally switched by the MAP instead of being tunneled back to an WX.

When applying a VLAN profile causes traffic that had been tunneled to an WX to be locally switched by MAPs, or vice-versa, the sessions of clients associated with the MAPs where the VLAN profile is applied are terminated, and the clients must re-associate with the MAPs.
Examples — The following command specifies that MAP 7 use VLAN profile `locals`:

```plaintext
WX# set ap 7 local-switching vlan-profile locals
success: change accepted.
```

See Also

- `clear ap local-switching vlan-profile` on page 355
- `set ap local-switching mode` on page 427
- `set vlan profile` on page 175

---

**set ap name**

Changes a MAP name.

**Syntax** — `set ap ap number name name`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `name` — Alphanumeric string of up to 16 characters, with no spaces.

**Defaults** — The default name of a directly attached MAP is based on the port number of the MAP access port attached to the MAP. For example, the default name for a MAP on MAP access port 1 is `MAP01`.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Default Distributed MAP name changed from `DMPnum` to `DAPnum` in MSS Version 4.1. Version 6.0 removed the `dap` option.

**Examples** — The following command changes the name of the MAP on port 1 to `techpubs`:

```plaintext
WX1200# set ap 1 name techpubs
success: change accepted.
```

See Also

- `display ap config` on page 364
set ap radio antenna-location

Specifies the location (indoors or outdoors) of an external antenna. Use this command to ensure that the proper set of channels is available on the radio. In some cases, the set of valid channels for a radio differs depending on the location of the antenna, indoors or outdoors.

**Syntax** — `set ap apnum radio number antenna-location {indoors | outdoors}`

- `ap apnum`—Index value that identifies the MAP on the WX.
- `radio number`—Specify radio 1 or radio 2.
- `antenna-location`—Specify antenna location.
- `indoors`—Specifies that the external antenna is installed indoors (inside the building).
- `outdoors`—Specifies that the external antenna is installed outdoors.

**Defaults** — The default antenna location is indoors.

**Access** — Enabled.

**History** — Introduced in MSS 5.0.

**Examples** — The following command sets the antenna location for radio 1 on Distributed MAP 22 to outdoors:

```
WX2200# set ap 22 radio 1 antenna-location outdoors
success: change accepted.
```

**See Also**

- `set ap radio antennatype` on page 431
set ap radio antennatype

Sets the model number for an external antenna.

**Syntax** — `set ap ap-number radio {1|2} antennatype {ANT1060 | ANT1120 | ANT1180 | ANT5060 | ANT5120 | ANT5180 | ANT-1360-OUT | ANT-5360-OUT | ANT-5120-OUT | internal}`

- **ap ap-number** — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **antennatype {ANT1060 | ANT1120 | ANT1180 | internal}** — 802.11b/g external antenna models:
  - **ANT1060** — 60° 802.11b/g antenna
  - **ANT1120** — 120° 802.11b/g antenna
  - **ANT1180** — 180° 802.11b/g antenna
  - **internal** — uses the internal antenna instead
- **antennatype {ANT5060 | ANT5120 | ANT5180 | internal}** — 802.11a external antenna models:
  - **ANT5060** — 60° 802.11a antenna
  - **ANT5120** — 120° 802.11a antenna
  - **ANT5180** — 180° 802.11a antenna
  - **internal** — uses the internal antenna instead
- **antennatype {ANT-1360-OUT | ANT5360-OUT | ANT5060 | ANT5120-OUT | internal}** — 802.11a external antenna models:
  - **ANT1360-OUT** — 360° 802.11b/g antenna
  - **ANT5360-OUT** — 360° 802.11a antenna
  - **ANT5060-OUT** — 60° 802.11a antenna
  - **ANT5120-OUT** — 120° 802.11a antenna
  - **internal** — uses the internal antenna instead
Defaults — All radios use the internal antenna by default, if the MAP model has an internal antenna. The AP 3150 802.11b/g radio uses model ANT1060 by default."

Access — Enabled.

History — Introduced in MSS Version 3.0. Model numbers added for 802.11a external antennas, and the default changed to internal (except for the AP3150) in MSS Version 3.2.

Examples — The following command configures the 802.11b/g radio on Distributed MAP 1 to use antenna model ANT1060:

```
WX4400# set ap 1 radio 1 antennatype ANT1060
success: change accepted.
```

See Also

- display ap config on page 364

---

**set ap radio auto-tune max-power**

Sets the maximum power that RF Auto-Tuning can set on a radio.

Syntax — set {ap ap-number auto} radio {1 | 2} auto-tune max-power power-level

- **ap ap-number** — Index value that identifies the MAP on the WX.
- **ap auto** — Sets the maximum power for radios configured by the MAP configuration profile. (See set ap auto on page 410.)
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **power-level** — Maximum power setting RF Auto-Tuning can assign to the radio, expressed as the number of decibels in relation to 1 milliwatt (dBm). You can specify a value from 1 up to the maximum value allowed for the country of operation.

The power-level can be a value from 1 to 20.
set ap radio auto-tune max-retransmissions

**Defaults** — The default maximum power setting that RF Auto-Tuning can set on a radio is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Option `auto` added for configuration of the MAP configuration profile.

**Examples** — The following command sets the maximum power that RF Auto-Tuning can set on radio 1 on the MAP access point on port 6 to 12 dBm.

```verbatim
WX1200# set ap 7 radio 1 auto-tune max-power 12
success: change accepted.
```

**See Also**
- `set ap radio auto-tune max-retransmissions` on page 433
- `set radio-profile auto-tune power-config` on page 454
- `set radio-profile auto-tune power-interval` on page 455

---

**set ap radio auto-tune max-retransmissions**

Sets the maximum percentage of client retransmissions a radio can experience before RF Auto-Tuning considers changing the channel on the radio. A high percentage of retransmissions is a symptom of interference on the channel.

**Syntax** — `set {ap ap-number auto} radio {1 | 2} auto-tune max-retransmissions retransmissions`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `ap auto` — Sets the maximum retransmissions for radios configured by the MAP configuration profile. (See `set ap auto` on page 410.)
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- `retransmissions` — Percentage of packets that can result in retransmissions without resulting in a channel change. You can specify from 1 to 100.
Defaults — The default is 10 percent.

Access — Enabled.

History — Introduced in MSS Version 3.0. Option auto added for configuration of the MAP configuration profile. Version 6.0 removed the dap option.

Usage — A retransmission is a packet sent from a client to a MAP radio that the radio receives more than once. This can occur when the client does not receive an 802.11 acknowledgement for a packet sent to the radio.

If the radio receives only a single copy of a packet that is transmitted multiple times by a client, the packet is not counted by the radio as a retransmission. For example, if a packet is corrupted and the radio does not receive it, but the second copy of the packet does reach the radio, the radio does not count the packet as a retransmission since the radio received only one recognizable copy of the packet.

The interval is 1000 packets. If more than the specified percentage of packets within a group of 1000 packets received by the radio are retransmissions, the radio increases power.

When the percentage of retransmissions exceeds the max-retransmissions threshold, the radio does not immediately increase power. Instead, if the data rate at which the radio is sending packets to the client is above the minimum data rate allowed, the radio lowers the data rate by one setting. If the retransmissions still exceed the maximum allowed, the radio continues to lower the data rate, one setting at a time, until either the retransmissions fall within the allowed percentile or the minimum allowed data rate is reached.

If the retransmissions still exceed the threshold after the minimum allowed data rate is reached, the radio increases power by 1 dBm. The radio continues increasing the power in 1 dBm increments until the retransmissions fall below the threshold.

After the retransmissions fall below the threshold, the radio reduces power by 1 dBm. As long as retransmissions remain below the threshold, the radio continues reducing power in 1 dBm increments until it returns to its default power level.
A radio also can increase power, in 1 dBm increments, if a client falls below the minimum allowed data rate. After a radio increases power, all clients must be at the minimum data rate or higher and the maximum retransmissions must be within the allowed percentile, before the radio begins reducing power again.

Examples — The following command changes the max-retransmissions value to 20:

```
WX1200# set ap 6 radio 1 auto-tune max-retransmissions 20
success: change accepted.
```

See Also

- `set ap radio auto-tune max-power` on page 432
- `set radio-profile auto-tune power-config` on page 454
- `set radio-profile auto-tune power-interval` on page 455

---

**set ap radio channel**

Sets a MAP radio's channel.

**Syntax** — `set ap port-list radio {1 | 2} channel channel-number`

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- `channel channel-number` — Channel number. The valid channel numbers depend on the country of operation.

**Defaults** — The default channel depends on the radio type:

- The default channel number for 802.11b/g is 6.
- The default channel number for 802.11a is the lowest valid channel number for the country of operation.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 6.0 removed the `dap` option.
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

Usage — You can configure the transmit power of a radio on the same command line. Use the tx-power option.

This command is not valid if dynamic channel tuning (RF Auto-Tuning) is enabled.

Examples — The following command configures the channel on the 802.11a radio on the MAP access point connected to port 5:

WX1200# set ap 5 radio 1 channel 36
success: change accepted.

The following command configures the channel and transmit power on the 802.11b/g radio on the MAP access point connected to port 1:

WX1200# set ap 1 radio 1 channel 1 tx-power 10
success: change accepted.

See Also

- display ap config on page 364
- set ap radio tx-power on page 441

---

`set ap radio link-calibration` Configures an MAP radio to emit link calibration packets, which can aid in positioning a Mesh AP.

**Syntax** — set ap `ap-number` radio {1 | 2} link-calibration

mode {enable | disable}

- `ap ap-number` — Index value that identifies the MAP on the WX.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- `mode enable` — Enables link calibration packets for the MAP radio.
- `mode disable` — Disables link calibration packets for the MAP radio.

**Defaults** — Disabled.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.
Usage — A Mesh Portal MAP can be configured to emit link calibration packets to assist with positioning the Mesh AP. A link calibration packet is an unencrypted 802.11 management packet of type Action. When enabled on an MAP, link calibration packets are sent at a rate of 5 per second.

Only one radio on an MAP can be configured to send link calibration packets. Link calibration packets are intended to be used only during installation of MAPs; they are not intended to be enabled on a continual basis.

Examples — The following command enables link calibration packets for MAP radio 1 on MAP 7:

```
WX# set ap 7 radio 1 link-calibration mode enable
WX#
```

See Also
- display ap mesh-links on page 377
- set ap boot-configuration mesh ssid on page 421
- set service-profile mesh on page 498

---

**set ap radio load balancing**

Disables or enables RF load balancing for an MAP radio.

Syntax — `set ap ap-number radio {1 | 2} load balancing {enable | disable}`

- `ap ap-number` — Index value that indentifies the MAP on the WX.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- `enable` — Enables link calibration packets for the MAP radio.
- `disable` — Disables link calibration packets for the MAP radio.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS Version 6.0.
**Usage** — By default, RF load balancing is enabled on all MAP radios. Use this command to disable or re-enable RF load balancing for the specified MAP radio.

RF load balancing can also be disabled or re-enabled globally with the `set load-balancing mode` command. If RF load balancing has been enabled or disabled for a specific MAP radio, then the setting for the individual radio takes precedence over the global setting.

**Examples** — The following command disables RF load balancing for MAP radio 1 on MAP 7:

```
WX# set ap 7 radio 1 load-balancing disable
WX#
```

**See Also**

- `set load-balancing strictness` on page 447
- `clear ap radio load-balancing group` on page 359
- `set ap local-switching mode` on page 427
- `display load-balancing group` on page 396

---

**set ap radio load balancing group**

Assigns an MAP radio to a load balancing group.

```
Syntax — set ap ap-number radio {1 | 2} load-balancing group name [rebalance]
```

- **ap ap-number** — Index value that identifies the MAP on the WX.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- **group name** — Name of an RF load balancing group to which the MAP radio is assigned. A radio can belong to only one group.
- **rebalance** — Configures the MAP radio to disassociate its client sessions and rebalance them whenever a new MAP radio is added to the load balancing group.

**Defaults** — By default, MAP radios are not part of an RF load balancing group.
Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Assigning radios to specific load balancing groups is optional. When you do this, MSS considers them to have exactly overlapping coverage areas, rather than using signal strength calculations to determine their overlapping coverage. MSS attempts to distribute client sessions across radios in the load balancing group evenly. A radio can be assigned to only one group.

Examples The following command assigns MAP radio 1 on MAP 7 to load balancing group room1:

\[WX\# \text{set ap 7 radio 1 load-balancing group room1}\]

See Also

- clear ap radio load-balancing group on page 359
- display load-balancing group on page 396
- set load-balancing strictness on page 447
- set ap local-switching mode on page 427

set ap radio mode

Enables or disables a radio on a MAP access point.

Syntax — \texttt{set ap \{ap-number \mid auto\} radio \{1 \mid 2\} mode \{enable \mid disable\}}

- \texttt{ap ap-number} — Index value that identifies the MAP on the WX.
- \texttt{radio 1} — Radio 1 of the MAP.
- \texttt{radio 2} — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- \texttt{mode enable} — Enables a radio.
- \texttt{mode disable} — Disables a radio.

Defaults — MAP access point radios are disabled by default.

Access — Enabled.
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

History — Introduced in MSS Version 3.0. Option auto added for configuration of the MAP configuration profile. Version 6.0 removed the dap option.

Usage — To enable or disable one or more radios to which a profile is assigned, use the set ap radio radio-profile command. To enable or disable all radios that use a specific radio profile, use the set radio-profile command.

Examples — The following command enables radio 1 on the MAP 1:

WX1200# set ap 1 radio 1 mode enable
success: change accepted.

The following command enables radio 2 on on MAP 1:

WX1200# set ap 1 radio 2 mode enable
success: change accepted.

See Also
- clear ap radio on page 356
- display ap config on page 364
- set ap radio radio-profile on page 440
- set radio-profile mode on page 464

---

**set ap radio radio-profile**

Assigns a radio profile to a MAP radio and enables or disables the radio.

**Syntax** — set ap {ap-number | auto} radio {1 | 2} radio-profile name mode {enable | disable}
- ap ap-number — Index value that identifies the MAP on the WX.
- radio 1 — Radio 1 of the MAP.
- radio 2 — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- radio-profile name — Radio profile name of up to 16 alphanumeric characters, with no spaces.
- mode enable — Enables radios on the specified ports with the parameter settings in the specified radio profile.
- mode disable — Disables radios on the specified ports.
**set ap radio tx-power**

Sets the transmit power of a MAP radio.

**Syntax** — \texttt{set ap \{ap-number\} radio \{1 \mid 2\} tx-power power-level}

- \texttt{ap ap-number} — Index value that identifies the MAP on the WX.
- \texttt{radio 1} — Radio 1 of the MAP.
- \texttt{radio 2} — Radio 2 of the MAP. (This option does not apply to single-radio models.)
- \texttt{tx-power power-level} — Number of decibels in relation to 1 milliwatt (dBm). The valid values depend on the country of operation.

The maximum transmit power you can configure on any 3Com radio is the maximum allowed for the country in which you plan to operate the radio or one of the following values if that value is less than the

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Option \texttt{auto} added for configuration of the MAP configuration profile. Version 6.0 removed the \texttt{dap} option.

**Usage** — When you create a new profile, the radio parameters in the profile are set to their factory default values.

To enable or disable all radios using a specific radio profile, use \texttt{set radio-profile}.

**Examples** — The following command enables radio 1 on MAP 5 assigned to radio profile \texttt{rp1}:

\begin{verbatim}
WX1200# set ap 5radio 1 radio-profile rp1 mode enable
success: change accepted.
\end{verbatim}

**See Also**
- \texttt{clear ap radio} on page 356
- \texttt{display radio-profile} on page 398
- \texttt{set ap radio mode} on page 439
- \texttt{set radio-profile mode} on page 464

country maximum: on an 802.11a radio, 11 dBm for channel numbers less than or equal to 64, or 10 dBm for channel numbers greater than 64; on an 802.11b/g radio, 16 dBm for all valid channel numbers for 802.11b, or 14 dBm for all valid channel numbers for 802.11g.

**Defaults** — The default transmit power on all MAP radio types is the highest setting allowed for the country of operation or highest setting supported on the hardware, whichever is lower.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 6.0 removed the dap option.

**Usage** — You also can configure a radio channel on the same command line. Use the channel option.

This command is not valid if dynamic power tuning (RF Auto-Tuning) is enabled.

**Examples** — The following command configures the transmit power on the 802.11a radio on the MAP access point connected to port 5:

```
WX1200# set ap 5 radio 1 tx-power 10
success: change accepted.
```

The following command configures the channel and transmit power on the 802.11b/g radio on the MAP access point connected to port 1:

```
WX1200# set ap 1 radio 1 channel 1 tx-power 10
success: change accepted.
```

**See Also**

- display ap config on page 364
- set ap radio channel on page 435
set ap security

Sets security requirements for management sessions between a WX and its Distributed MAPs.

This feature applies to Distributed MAPs only, not to directly connected MAPs configured on MAP access ports.

The maximum transmission unit (MTU) for encrypted MAP management traffic is 1498 bytes, whereas the MTU for unencrypted management traffic is 1474 bytes. Make sure the devices in the intermediate network between the WX switch and Distributed MAP can support the higher MTU.

Syntax — `set ap security secsetting {require | optional | none}

- `security secsetting` — Name of the security setting.
- `require` — Requires all Distributed MAPs to have encryption keys that have been verified in the CLI by an administrator. If a MAP does not have an encryption key or the key has not been verified, the WX does not establish a management session with the MAP.
- `optional` — Allows MAPs to be managed by the switch even if they do not have encryption keys or their keys have not been verified by an administrator. Encryption is used for MAPs that support it.
- `none` — Encryption is not used, even for MAPs that support it.

Defaults — The default setting is `optional`.

Access — Enabled.

History — Introduced in MSS 4.0. Version 6.0 removed the `dap` option.

Usage — This parameter applies to all Distributed MAPs managed by the WX. If you change the setting to `required`, the WX requires Distributed MAPs to have encryption keys. The WX also requires their fingerprints to be verified in MSS. When MAP security is required, a MAP can establish a management session with the WX only if its fingerprint has been verified by you in MSS.

A change to MAP security support does not affect management sessions that are already established. To apply the new setting to a MAP, restart the MAP.
Examples — The following command configures a WX to require Distributed MAPs to have encryption keys:

```
WX4400# set ap security require
```

See Also

- display ap config on page 364
- display ap status on page 379
- set ap fingerprint on page 424

---

**set ap upgrade-firmware**

Disables or reenables automatic upgrade of a MAP access point boot firmware.

**Syntax** — `set ap auto upgrade-firmware {enable | disable}`

- **ap auto** — Configures firmware upgrades for the MAP configuration profile (See “set ap auto” on page 410.)
- **enable** — Enables automatic firmware upgrades.
- **disable** — Disables automatic firmware upgrades.

**Defaults** — Automatic firmware upgrades of MAP access points are enabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Option `auto` added for configuration of the MAP configuration profile. Version 6.0 removed the `dap` option.

**Usage** — When the feature is enabled on an WX port, a MAP access point connected to that port upgrades its boot firmware to the latest version stored on the WX switch.

**Examples** — The following command disables automatic firmware upgrades on the MAP access point connected to port 6:

```
WX1200# set ap 6 upgrade-firmware disable
```

See Also

- display ap config on page 364
set band-preference

Configures MSS to steer clients that support both the 802.11a and 802.11b/g radio bands to a specific radio on an MAP for the purpose of RF load balancing.

**Syntax** — set band-preference {none | 11bg | 11a}

- **none** — When a client supports both 802.11a and 802.11b/g radio bands, does not steer the client to a specific MAP radio.
- **enable** — When a client supports both 802.11a and 802.11b/g radio bands, steers the client to the 802.11b/g radio.
- **disable** — When a client supports both 802.11a and 802.11b/g radio bands, steers the client to the 802.11a radio.

**Defaults** — By default, clients are not steered to specific MAP radios for RF load balancing.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — Use this command to steer clients that support both the 802.11a and 802.11b/g bands, to a specific radio on an MAP for the purpose of load balancing. This global band-preference option controls the degree that an MAP with two radios attempts to conceal one of its radios from a client with the purpose of steering the client to the other radio.

**Examples** — The following command steers clients that support both the 802.11a and 802.11b/g bands to the 802.11a radio on an MAP:

```
WX# set band-preference 11a
WX#
```

**See Also**

- display load-balancing group on page 396
- set load-balancing mode on page 446
- set load-balancing strictness on page 447
- set ap radio load balancing on page 437
set load-balancing mode

Disables or reenables RF load balancing globally on the WXMAP.

**Syntax** — set load-balancing mode {enable | disable}

- `enable` — Enables RF load balancing globally on the WX.
- `disable` — Disables RF load balancing globally on the WX.

**Defaults** — RF load balancing is enabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — By default, RF load balancing is enabled on all MAP radios. Use this command to disable or re-enable RF load balancing globally for all MAP radios managed by the WX.

If RF load balancing has been enabled or disabled for a specific MAP radio, then the setting for the individual radio takes precedence over the global setting.

**Examples** — The following command globally disables RF load balancing for all MAP radios managed by the WX switch:

```
WX# set load-balancing mode disable
WX#
```

**See Also**

- `display load-balancing group` on page 396
- `set load-balancing strictness` on page 447
- `set band-preference` on page 445
- `set ap radio load balancing` on page 437
**set load-balancing strictness** Controls the degree to which MSS balances the client load among MAPs when performing RF load balancing.

**Syntax** — `set load-balancing strictness {low | med | high | max}`

- **low** — No clients are denied service. New clients can be steered to other MAPs, but only to the extent that service can be provided to all clients.
- **med** — Overloaded radios steer new clients to other MAPs more strictly than the low option. Clients attempting to connect to overloaded radios may be delayed several seconds.
- **high** — Overloaded radios steer new clients to other MAPs more strictly than the med option. Clients attempting to connect to overloaded radios may be delayed up to a minute.
- **max** — RF load balancing is strictly enforced. That is, overloaded radios do not respond to new clients at all. A client would not be able to connect during times that all of the detectable MAP radios are overloaded.

**Defaults** — Low.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — When performing RF load balancing, MSS may attempt to steer clients to less-busy radios in a load-balancing group. To do this, MSS makes MAP radios with heavy client loads less visible to new clients, causing them to associate with MAP radios that have a lighter load.

Use this command to specify how strictly MSS attempts to keep the client load balanced across the MAP radios in the load-balancing group. When low strictness is specified (the default), MSS makes heavily loaded MAP radios less visible in order to steer clients to less-busy MAP radios, but ensures that even if all the MAP radios in the group are heavily loaded, clients are not denied service.
At the other end of the spectrum, when max strictness is specified, if an MAP radio has reached its maximum client load, MSS makes it invisible to new clients, causing them to attempt to connect to other MAP radios. In the event that all the MAP radios in the group have reached their maximum client load, then no new clients would be able to connect to the network.

**Examples** The following command sets the RF load balancing strictness to the maximum setting:

```bash
WX# set load-balancing strictness max
Success: strictness set to "MAX"
```

**See Also**
- `display load-balancing group` on page 396
- `set load-balancing mode` on page 446
- `set band-preference` on page 445
- `set ap radio load balancing` on page 437

---

**set radio-profile 11g-only**
Deprecated in MSS Version 4.2. To configure radio data rates, see `set service-profile transmit-rates` on page 516.

**set radio-profile active-scan**
Disables or reenables active RF detection scanning on the MAP radios managed by a radio profile. When scanning is enabled, MAP radios look for rogue devices by sending `probe any` requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Passive scanning is always enabled and cannot be disabled. During passive scanning, radios look for rogues by listening for beacons and probe responses.

**Syntax** — `set radio-profile name active-scan {enable | disable}`

- `name` — Radio profile name.
- `enable` — Configures radios to actively scan for rogues.
set radio-profile auto-tune 11a-channel-range

- **disable** — Configures radios to scan only passively for rogues by listening for beacons and probe responses.

**Defaults** — Active scanning is enabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — You can enter this command on any WX in the Mobility Domain. The command takes effect only on that WX.

**Examples** — The following command disables active scan in radio profile *radprof3*:

```
wx4400# set radio-profile radprof3 active-scan disable
success: change accepted.
```

**See Also**

- **display radio-profile** on page 398

---

**set radio-profile auto-tune 11a-channel-range** When configured, the MAP 802.11a radio selects a channel from a limited range of available channels or all available channels.

**Syntax** — `set radio-profile name auto-tune 11a-channel-range {lower-bands | all-bands}

- **name** — The name of the radio profile to configure the 802.11a channel range.
- **lower-bands** — Only the lower channels are available for the 802.11a radio: 36, 40, 44, 48, 52, 56, 60, or 64.
- **all-bands** — All 802.11a channels are available for the 802.11a radio: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, and 161.

**Defaults** — None

**Access** — Enabled

**History** — Version 6.0Command introduced.

**Usage** — Improves the 802.11a radio usage on the network.
Examples — The following command enables the 802.11a radio to select any available channel in the 802.11a range:

WX1200# set radio-profile test auto-tune 11a-channel-range all-bands
success: change accepted.

set radio-profile auto-tune channel-config

Disables or reenables dynamic channel tuning (RF Auto-Tuning) for the MAP radios in a radio profile.

Syntax — set radio-profile name auto-tune channel-config
{enable | disable}[ignore-client]

- name — Radio profile name.
- enable — Configures radios to dynamically select their channels when the radios are started.
- disable — Configures radios to use their statically assigned channels, or the default channels if unassigned, when the radios are started.
- ignore-clients — Configures radios to change channels regardless of client status. Without this option, a radio changes the channel only if the radio does not have any active clients on that channel.

Defaults — Dynamic channel assignment is enabled by default.

Access — Enabled.


Usage — If you disable RF Auto-Tuning for channels, MSS does not dynamically set the channels when radios are first enabled and also does not tune the channels during operation.

If RF Auto-Tuning for channels is enabled, MSS does not allow you to manually change channels.

RF Auto-Tuning of channels on 802.11a radios uses only the bottom eight channels in the band (36, 40, 44, 48, 52, 56, 60, and 64). To use a higher channel number, you must disable RF Auto-Tuning of channels on the radio profile the radio is in, and use the set ap | radio channel command to statically configure the channel.
Examples — The following command disables dynamic channel tuning for radios in the rp2 radio profile:

```
WX4400# set radio-profile rp2 auto-tune channel-config disable
success: change accepted.
```

See Also

- `display radio-profile` on page 398
- `set ap radio channel` on page 435
- `set radio-profile auto-tune channel-holddown` on page 451
- `set radio-profile auto-tune channel-interval` on page 452
- `set radio-profile auto-tune power-config` on page 454

---

**set radio-profile auto-tune channel-holddown**

Sets the minimum number of seconds a radio in a radio profile must remain at its current channel assignment before RF Auto-Tuning can change the channel. The channel holddown provides additional stability to the network by preventing the radio from changing channels too rapidly in response to spurious RF anomalies such as short-duration channel interference.

**Syntax** — `set radio-profile name auto-tune channel-holddown holddown`

- `name` — Radio profile name.
- `holddown` — Minimum number of seconds a radio must remain on its current channel setting before RF Auto-Tuning is allowed to change the channel. You can specify from 0 to 65535 seconds.

**Defaults** — The default RF Auto-Tuning channel holddown is 900 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — The channel holddown applies even if RF anomalies occur that normally cause an immediate channel change.
Examples — The following command changes the channel holddown for radios in radio profile rp2 to 600 seconds:

```
WX4400# set radio-profile rp2 auto-tune channel-holddown 600
success: change accepted.
```

See Also

- *display radio-profile* on page 398
- *set radio-profile auto-tune channel-config* on page 450
- *set radio-profile auto-tune channel-lockdown* on page 453

---

**set radio-profile auto-tune channel-interval**

Sets the interval at which RF Auto-Tuning decides whether to change the channels on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio channels if needed.

**Syntax** — set radio-profile name auto-tune channel-interval seconds

- **name** — Radio profile name.
- **seconds** — Number of seconds RF Auto-Tuning waits before changing radio channels to adjust to RF changes, if needed. You can specify from 0 to 65535 seconds.

**Defaults** — The default channel interval is 3600 seconds (one hour).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — 3Com recommends that you use an interval of at least 300 seconds (5 minutes).

RF Auto-Tuning can change a radio’s channel before the channel interval expires in response to RF anomalies. Even in this case, channel changes cannot occur more frequently than the channel holddown interval.

If you set the interval to 0, RF Auto-Tuning does not reevaluate the channel at regular intervals. However, RF Auto-Tuning can still change the channel in response to RF anomalies.
Examples — The following command sets the channel interval for radios in radio profile `rp2` to 2700 seconds (45 minutes):

```plaintext
WX4400# set radio-profile rp2 auto-tune channel-interval 2700
success: change accepted.
```

See Also
- `display radio-profile` on page 398
- `set radio-profile auto-tune channel-config` on page 450
- `set radio-profile auto-tune channel-holddown` on page 451

**set radio-profile auto-tune channel-lockdown**

Locks down the current channel settings on all radios in a radio profile. The channel settings that are in effect when the command is entered are changed into statically configured channel assignments on the radios. RF Auto-Tuning of channels is then disabled in the radio profile.

**Syntax** — `set radio-profile name auto-tune channel-lockdown`

- `name` — Radio profile name.

**Defaults** — By default, when RF Auto-Tuning of channels is enabled, channels continue to be changed dynamically based on network conditions.

**Access** — Enabled.

**History** — Introduced in MSS Version 5.0.

**Usage** — To save this command and the static channel configuration commands created when you enter this command, save the configuration.
**Examples** — The following command locks down the channel settings for radios in radio profile *rp2*:

```
WX# set radio-profile rp2 auto-tune channel-lockdown
success: change accepted
```

**See Also**

- `display radio-profile` on page 398
- `set radio-profile auto-tune channel-config` on page 450
- `set radio-profile auto-tune channel-holddown` on page 451
- `set radio-profile auto-tune channel-interval` on page 452
- `set radio-profile auto-tune channel-config` on page 450

---

**set radio-profile auto-tune power-config**

Enables or disables dynamic power tuning (RF Auto-Tuning) for the MAP radios in a radio profile.

**Syntax** — `set radio-profile name auto-tune power-config {enable | disable}`

- `name` — Radio profile name.
- `enable` — Configures radios to dynamically set their power levels when the MAPs are started.
- `disable` — Configures radios to use their statically assigned power levels, or the default power levels if unassigned, when the radios are started.

**Defaults** — Dynamic power assignment is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — When RF Auto-Tuning for power is disabled, MSS does not dynamically set the power levels when radios are first enabled and also does not tune power during operation with associated clients.

When RF Auto-Tuning for power is enabled, MSS does not allow you to manually change the power level.
**Examples** — The following command enables dynamic power tuning for radios in the *rp2* radio profile:

```
WX4400# set radio-profile rp2 auto-tune power-config enable
success: change accepted.
```

**See Also**
- `display radio-profile` on page 398
- `set ap radio auto-tune max-power` on page 432
- `set ap radio auto-tune max-retransmissions` on page 433
- `set radio-profile auto-tune channel-config` on page 450
- `set radio-profile auto-tune power-interval` on page 455

---

**set radio-profile auto-tune power-interval**

Sets the interval at which RF Auto-Tuning decides whether to change the power level on radios in a radio profile. At the end of each interval, MSS processes the results of the RF scans performed during the previous interval, and changes radio power levels if needed.

**Syntax** — `set radio-profile name auto-tune power-interval seconds`

- `name` — Radio profile name.
- `seconds` — Number of seconds MSS waits before changing radio power levels to adjust to RF changes, if needed. You can specify from 1 to 65535 seconds.

**Defaults** — The default power tuning interval is 600 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command sets the power interval for radios in radio profile *rp2* to 240 seconds:

```
WX4400# set radio-profile rp2 auto-tune power-interval 240
success: change accepted.
```
**set radio-profile auto-tune power-lockdown**

Locks down the current power settings on all radios in a radio profile. The power settings that are in effect when the command is entered are changed into statically configured power settings on the radios. RF Auto-Tuning of power is then disabled in the radio profile.

**Syntax** — set radio-profile name auto-tune power-lockdown

- **name**—Radio profile name.

**Defaults** — By default, when RF Auto-Tuning of power is enabled, power settings continue change dynamically based on network conditions.

**Access** — Enabled.

**History** — Introduced in MSS Version 5.0.

**Usage** — To save this command and the static power configuration commands created when you enter this command, save the configuration.

**Examples** — The following command locks down the power settings for radios in radio profile rp2:

```
WX1200# set radio-profile rp2 auto-tune power-lockdown
success: change accepted.
```

**See Also**

- set ap radio auto-tune max-power on page 432
- set radio-profile auto-tune channel-lockdown on page 453
- set radio-profile auto-tune power-config on page 454
- set radio-profile auto-tune power-interval on page 455
- set radio-profile auto-tune power-ramp-interval on page 457
- display radio-profile on page 398
set radio-profile auto-tune power-ramp-interval

Changes the interval at which power is increased or decreased, in 1 dBm increments, on radios in a radio profile until the optimum power level calculated by RF Auto-Tuning is reached.

Syntax — set radio-profile name auto-tune power-ramp-interval seconds

- **name** — Radio profile name.
- **seconds** — Number of seconds MSS waits before increasing or decreasing radio power by another 1 dBm. You can specify from 1 to 65535.

Defaults — The default interval is 60 seconds.

Access — Enabled.

History — Introduced in MSS Version 5.0.

Examples — The following command changes the power ramp interval for radios in radio profile rp2 to 120 seconds:

```plaintext
WX1200# set radio-profile rp2 auto-tune power-ramp-interval 120
success: change accepted.
```

See Also

- set ap radio auto-tune max-power on page 432
- set radio-profile auto-tune power-config on page 454
- set radio-profile auto-tune power-interval on page 455
- set radio-profile auto-tune power-ramp-interval on page 457
- display radio-profile on page 398

set radio-profile beacon-interval

Changes the rate at which each MAP radio in a radio profile advertises its service set identifier (SSID).

Syntax — set radio-profile name beacon-interval interval

- **name** — Radio profile name.
- **interval** — Number of milliseconds (ms) between beacons. You can specify from 25 ms to 8191 ms.

Defaults — The beacon interval for MAP radios is 100 ms by default.
Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the `set radio-profile mode` command.

Examples — The following command changes the beacon interval for radio profile `rp1` to 200 ms:

```
WX4400# set radio-profile rp1 beacon-interval 200
success: change accepted.
```

See Also
- `display radio-profile` on page 398
- `set radio-profile mode` on page 464

---

**set radio-profile countermeasures**

Enables or disables countermeasures on the MAP radios managed by a radio profile. Countermeasures are packets sent by a radio to prevent clients from being able to use rogue access points.

⚠️ **CAUTION:** Countermeasures affect wireless service on a radio. When a MAP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.

MAP radios can also issue countermeasures against interfering devices. An interfering device is not part of the 3Com network but also is not a rogue. No client connected to the device has been detected communicating with any network entity listed in the forwarding database (FDD) of any WX in the Mobility Domain. Although the interfering device is not connected to your network, the device might be causing RF interference with MAP radios.

**Syntax** — `set radio-profile name countermeasures {all | rogue | configured | none}`

- `name` — Radio profile name.
- `all` — Configures radios to attack rogues and interfering devices.
- `rogue` — Configures radios to attack rogues only.
set radio-profile countermeasures

- **configured** — Configures radios to attack only devices in the attack list on the WX switch (on-demand countermeasures). When this option is specified, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.

- **none** — Disables countermeasures for this radio profile.

**Defaults** — Countermeasures are disabled by default.

**Access** — Enabled.

**History** — Command introduced in MSS Version 4.0. New option **configured** added to support on-demand countermeasures in MSS Version 4.1.

**Examples** — The following command enables countermeasures in radio profile **radprof3** for rogues only:

```
WX1200# set radio-profile radprof3 countermeasures rogue
success: change accepted.
```

The following command disables countermeasures in radio profile **radprof3**:

```
WX1200# clear radio-profile radprof3 countermeasures
success: change accepted.
```

The following command causes radios managed by radio profile **radprof3** to issue countermeasures against devices in the WX switch’s attack list:

```
WX1200# set radio-profile radprof3 countermeasures configured
success: change accepted.
```

Note that when you issue this command, countermeasures are then issued only against devices in the WX attack list, not against other devices that were classified as rogues by other means.

**See Also**

- **display radio-profile** on page 398
set radio-profile dtim-interval

Changes the number of times after every beacon that each MAP radio in a radio profile sends a delivery traffic indication map (DTIM). A MAP sends the multicast and broadcast frames stored in its buffers to clients who request them in response to the DTIM.

The DTIM interval applies to both the beaconed SSID and the nonbeaconed SSID.

Syntax — set radio-profile name dtim-interval interval

- name — Radio profile name.
- interval — Number of times the DTIM is transmitted after every beacon. You can enter a value from 1 through 31.

Defaults — By default, MAP access points send the DTIM once after each beacon.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the set radio-profile mode command.

The DTIM interval does not apply to unicast frames.

Examples — The following command changes the DTIM interval for radio profile rp1 to 2:

WX4400# set radio-profile rp1 dtim-interval 2
success: change accepted.

See Also
- display radio-profile on page 398
- set radio-profile mode on page 464
set radio-profile frag-threshold

Changes the fragmentation threshold for the MAP radios in a radio profile. The fragmentation threshold is the threshold at which the long-retry-count is applicable instead of the short-retry-count.

The long-retry-count specifies the number of times a radio can send a unicast frame that is equal to or longer than the frag-threshold without receiving an acknowledgment.

The short-retry-count specifies the number of times a radio can send a unicast frame that is shorter than the frag-threshold without receiving an acknowledgment.

Syntax — set radio-profile name frag-threshold threshold

- name — Radio profile name.
- threshold — Maximum frame length, in bytes. You can enter a value from 256 through 2346.

Defaults — The default fragmentation threshold for MAP radios is 2346 bytes.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios using a radio profile before you can change parameters in the profile. Use the set radio-profile mode command.

The frag-threshold does not specify the maximum length a frame is allowed to be without being broken into multiple frames before transmission. The MAPs do not support fragmentation upon transmission, only upon reception.

The frag-threshold does not change the RTS threshold, which specifies the maximum length of a frame before the radio uses the RTS/CTS method to send the frame. To change the RTS threshold, use the set radio-profile rts-threshold command instead.

Examples — The following command changes the fragmentation threshold for radio profile rp1 to 1500 bytes:

WX4400# set radio-profile rp1 frag-threshold 1500
success: change accepted.
See Also
- `display radio-profile` on page 398
- `set radio-profile mode` on page 464
- `set radio-profile rts-threshold` on page 471
- `set service-profile long-retry-count` on page 497
- `set service-profile short-retry-count` on page 504

---

**set radio-profile**

**long-retry**

Deprecated in MSS Version 4.2. In 4.2, this parameter is associated with service profiles instead of radio profiles. See `set service-profile long-retry-count` on page 497.

---

**set radio-profile**

**max-rx-lifetime**

Changes the maximum receive threshold for the MAP radios in a radio profile. The maximum receive threshold specifies the number of milliseconds that a frame received by a radio can remain in buffer memory.

**Syntax** — `set radio-profile name max-rx-lifetime time`

- `name` — Radio profile name.
- `time` — Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

**Defaults** — The default maximum receive threshold for MAP radios is 2000 ms (2 seconds).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the `set radio-profile mode` command.

**Examples** — The following command changes the maximum receive threshold for radio profile `rpl` to 4000 ms:

```
WX4400# set radio-profile rpl max-rx-lifetime 4000
success: change accepted.
```
set radio-profile max-tx-lifetime

Changes the maximum transmit threshold for the MAP radios in a radio profile. The maximum transmit threshold specifies the number of milliseconds that a frame scheduled to be transmitted by a radio can remain in buffer memory.

**Syntax** — `set radio-profile name max-tx-lifetime time`

- `name` — Radio profile name.
- `time` — Number of milliseconds. You can enter a value from 500 (0.5 second) through 250,000 (250 seconds).

**Defaults** — The default maximum transmit threshold for MAP radios is 2000 ms (2 seconds).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the `set radio-profile mode` command.

**Examples** — The following command changes the maximum transmit threshold for radio profile `rp1` to 4000 ms:

```
WX4400# set radio-profile rp1 max-tx-lifetime 4000
success: change accepted.
```

**See Also**

- `display radio-profile` on page 398
- `set radio-profile mode` on page 464
- `set radio-profile max-tx-lifetime` on page 463
set radio-profile
mode

Creates a new radio profile, and disables or reenables all MAP radios that are using a specific profile.

**Syntax** — `set radio-profile name [mode {enable | disable}]`

- **radio-profile name** — Radio profile name of up to 16 alphanumeric characters, with no spaces.

*Use this command without the mode enable or mode disable option to create a new profile.*

- **mode enable** — Enables the radios that use this profile.
- **mode disable** — Disables the radios that use this profile.

**Defaults** — Each radio profile that you create has a set of properties with factory default values that you can change with the other `set radio-profile` commands in this chapter.

Table 73 lists the parameters controlled by a radio profile and their default values.

**Table 73  Defaults for Radio Profile Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Radio Behavior When Parameter Set to Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>active-scan</td>
<td>enable</td>
<td>Sends <em>probe any</em> requests (probe requests with a null SSID name) to solicit probe responses from other access points.</td>
</tr>
<tr>
<td>auto-tune</td>
<td>enable</td>
<td>Allows dynamic configuration of channel and power settings by MSS.</td>
</tr>
<tr>
<td>beacon-interval</td>
<td>100</td>
<td>Waits 100 ms between beacons.</td>
</tr>
<tr>
<td>countermeasures</td>
<td>Not configured</td>
<td>Does not issue countermeasures against any device.</td>
</tr>
<tr>
<td>dtim-interval</td>
<td>1</td>
<td>Sends the delivery traffic indication map (DTIM) after every beacon.</td>
</tr>
<tr>
<td>frag-threshold</td>
<td>2346</td>
<td>Uses the short-retry-count for frames shorter than 2346 bytes and uses the long-retry-count for frames that are 2346 bytes or longer.</td>
</tr>
<tr>
<td>max-rx-lifetime</td>
<td>2000</td>
<td>Allows a received frame to stay in the buffer for up to 2000 ms (2 seconds).</td>
</tr>
</tbody>
</table>
## Access

Enabled.

## History

Introduced in MSS Version 3.0. Version 4.2 made the following changes:

- Removed the following parameters that no longer apply:
  - 11g-only
  - long-retry
  - short-retry

- The wmm parameter name changed to qos-mode.

## Usage

Use the command without any optional parameters to create new profile. If the radio profile does not already exist, MSS creates a new radio profile. Use the **enable** or **disable** option to enable or disable all the radios using a profile. To assign the profile to one or more radios, use the **set ap radio radio-profile** command.

### Table 73 Defaults for Radio Profile Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Radio Behavior When Parameter Set to Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-tx-lifetime</td>
<td>2000</td>
<td>Allows a frame that is scheduled for transmission to stay in the buffer for up to 2000 ms (2 seconds).</td>
</tr>
<tr>
<td>preamble-length</td>
<td>short</td>
<td>Advertises support for short 802.11b preambles, accepts either short or long 802.11b preambles, and generates unicast frames with the preamble length specified by the client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This parameter applies only to 802.11b/g radios.</td>
</tr>
<tr>
<td>qos-mode</td>
<td>wmm</td>
<td>Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of MAP radios for Wi-Fi Multimedia (WMM).</td>
</tr>
<tr>
<td>rts-threshold</td>
<td>2346</td>
<td>Transmits frames longer than 2346 bytes by means of the Request-to-Send/Clear-to-Send (RTS/CTS) method.</td>
</tr>
<tr>
<td>service-profile</td>
<td>No service profiles defined</td>
<td>You must configure a service profile. The service profile sets the SSID name and other parameters.</td>
</tr>
</tbody>
</table>
To change a parameter in a radio profile, you must first disable all the radios in the profile. After you complete the change, you can reenable the radios.

To enable or disable specific radios without disabling all of them, use the `set ap radio` command.

**Examples** — The following command configures a new radio profile named `rp1`:

```
WX4400# set radio-profile rp1
success: change accepted.
```

The following command enables the radios that use radio profile `rp1`:

```
WX4400# set radio-profile rp1 mode enable
```

The following commands disable the radios that use radio profile `rp1`, change the beacon interval, then reenable the radios:

```
WX4400# set radio-profile rp1 mode disable
WX4400# set radio-profile rp1 beacon-interval 200
WX4400# set radio-profile rp1 mode enable
```

The following command enables the WPA IE on MAP radios in radio profile `rp2`:

```
WX4400# set radio-profile rp2 wpa-ie enable
success: change accepted.
```

**See Also**

- `display ap config` on page 364
- `display radio-profile` on page 398
- `set ap radio mode` on page 439
- `set ap radio radio-profile` on page 440
Changes the preamble length for which an 802.11b/g MAP radio advertises support. This command does not apply to 802.11a.

**Syntax** — `set radio-profile name preamble-length {long | short}

- `name` — Radio profile name.
- `long` — Advertises support for long preambles.
- `short` — Advertises support for short preambles.

**Defaults** — The default is `short`.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Changing the preamble length value affects only the support advertised by the radio. Regardless of the preamble length setting (`short` or `long`), an 802.11b/g radio accepts and can generate 802.11b/g frames with either short or long preambles.

If a client associated with an 802.11b/g radio uses long preambles for unicast traffic, the MAP still accepts frames with short preambles but does not transmit frames with short preambles. This change also occurs if the access point overhears a beacon from an 802.11b/g radio on another access point that indicates the radio has clients that require long preambles.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the `set radio-profile mode` command.

**Examples** — The following command configures 802.11b/g radios that use the radio profile `rp_long` to advertise support for long preambles instead of short preambles:

```
WX4400# set radio-profile rp_long preamble-length long
success: change accepted.
```

**See Also**
- `display radio-profile` on page 398
- `set radio-profile mode` on page 464
set radio-profile qos-mode

Sets the prioritization mode for forwarding queues on MAP radios managed by the radio profile.

Syntax — set radio-profile name qos-mode {svp | wmm}

- **svp** — Optimizes forwarding prioritization of MAP radios for SpectraLink Voice Priority (SVP).
- **wmm** — Classifies and marks traffic based on 802.1p and DSCP, and optimizes forwarding prioritization of MAP radios for Wi-Fi Multimedia (WMM).

**Defaults** — The default QoS mode is **wmm**.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — When SVP is enabled, MAP forwarding prioritization is optimized for SpectraLink Voice Priority (SVP) instead of WMM, and the MAP does not tag packets sent to the WX. Otherwise, classification and tagging remain in effect. (For information, see the “Configuring Quality of Service” chapter of the *Wireless LAN Switch and Controller Configuration Guide*.)

If you plan to use SVP or another non-WMM type of prioritization, you must configure ACLs to tag the packets. (See the “Enabling Prioritization for Legacy Voice over IP” section in the “Configuring and Managing Security ACLs” chapter of the *Wireless LAN Switch and Controller Configuration Guide*.)

**Examples** — The following command changes the QoS mode for radio profile *rp1* to SVP:

```
WX4400# set radio-profile rp1 qos-mode svp
success: change accepted.
```

**See Also**

- **display radio-profile** on page 398
- **set radio-profile mode** on page 464
**set radio-profile rfid-mode**

Enables MAP radios managed by a radio profile to function as location receivers in an AeroScout Visibility System. An AeroScout Visibility System allows system administrators to track mobile assets using RFID tags.

When you enable RFID mode on a radio profile, radios in the profile can receive and process signals transmitted by RFID tags and relay them with related information to the AeroScout Engine. If the floor plan is modeled in 3WXM, you also can use 3WXM to display the locations of assets.

**Syntax** — `set radio-profile name rfid-mode {enable | disable}`

- `name`—Radio profile name.
- `enable`—Enables radios to function as asset location receivers.
- `disable`—Disables radios from functioning as asset location receivers.

**Defaults** — The default is disable.

**Access** — Enabled.

**History** — Introduced in MSS Version 5.0.

**Examples** — The following command enables radios managed by radio profile `rp1` to act as asset location receivers:

```
WX1200# set radio-profile rp1 rfid-mode enable
success: change accepted.
```

**See Also**

- `set radio-profile mode` on page 464
- `display radio-profile` on page 398

---

**set radio-profile rate-enforcement**

Configures MSS to enforce data rates, which means that a connecting client must transmit at one of the mandatory or standard rates in order to associate with the MAP.

**Syntax** — `set radio-profile name rate-enforcement {enable | disable}`

- `name` — Radio profile name.
- `enable` — Enables data rate enforcement for the radios in the radio profile.
- `disable` — Disables data rate enforcement for the radios in the radio profile.
Defaults — Data rate enforcement is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Each type of radio (802.11a, 802.11b, and 802.11g) providing service to an SSID has a set of radio rates allowed for use when sending beacons, multicast frames, and unicast data. You can configure the rate set for each type of radio, specifying rates in three categories:

Mandatory - Valid 802.11 transmit rates that clients must support in order to associate with the MAP.

Disabled - Valid 802.11 transmit rates are disabled. MAPs do not transmit at the disabled rates.

Standard - Valid 802.11 transmit rates that are not disabled and are not mandatory.

By default, the rate set is not enforced, meaning that a client can associate with and transmit data to the MAP using a disabled data rate, although the MAP does not transmit data back to the client at the disabled rate.

You can use this command to enforce the data rates, which means that a connecting client must transmit at one of the mandatory or standard rates in order to associate with the MAP. When data rate enforcement is enabled, clients transmitting at the disabled rates are not allowed to associate with the MAP.

This command is useful if you want to completely prevent clients from transmitting at disabled data rates. For example, you can disable slower data rates so that clients transmitting at these rates do not consume bandwidth on the channel at the expense of clients transmitting at faster rates.

Examples — The following command enables data rate enforcement for radio profile rp1:

```
WX# set radio-profile rp1 rate-enforcement mode enable
success: change accepted.
```
set radio-profile rts-threshold

Changes the RTS threshold for the MAP radios in a radio profile. The RTS threshold specifies the maximum length a frame can be before the radio uses the RTS/CTS method to send the frame. The RTS/CTS method clears the air of other traffic to avoid corruption of the frame due to a collision with another frame.

Syntax — set radio-profile name rts-threshold threshold

- name — Radio profile name.
- threshold — Maximum frame length, in bytes. You can enter a value from 256 through 3000.

Defaults — The default RTS threshold for a MAP radio is 2346 bytes.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must disable all radios that are using a radio profile before you can change parameters in the profile. Use the set radio-profile mode command.

Examples — The following command changes the RTS threshold for radio profile rp1 to 1500 bytes:

WX4400# set radio-profile rpl rts-threshold 1500
success: change accepted.

See Also

- display radio-profile on page 398
- set radio-profile mode on page 464
set radio-profile service-profile

Maps a service profile to a radio profile. All radios that use the radio profile also use the parameter settings, including SSID and encryption settings, in the service profile.

**Syntax** — set radio-profile *name* service-profile *name*

- radio-profile *name* — Radio profile name of up to 16 alphanumeric characters, with no spaces.
- service-profile *name* — Service profile name of up to 16 alphanumeric characters, with no spaces.

**Defaults** — A radio profile does not have a service profile associated with it by default. In this case, the radios in the radio profile use the default settings for parameters controlled by the service profile. Table 74 lists the parameters controlled by a service profile and their default values.

**Table 74** Defaults for Service Profile Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Radio Behavior When Parameter Set to Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>attr</td>
<td>No attributes configured</td>
<td>Does not assign the SSID’s authorization attribute values to SSID users, even if attributes are not otherwise assigned.</td>
</tr>
<tr>
<td>auth-dot1x</td>
<td>enable</td>
<td>When the Wi-Fi Protected Access (WPA) information element (IE) is enabled, uses 802.1X to authenticate WPA clients.</td>
</tr>
<tr>
<td>auth-fallthru</td>
<td>web-auth</td>
<td>Uses WebAAA for users who do not match an 802.1X or MAC authentication rule for the SSID requested by the user.</td>
</tr>
<tr>
<td>auth-psk</td>
<td>disable</td>
<td>Does not support using a preshared key (PSK) to authenticate WPA clients.</td>
</tr>
<tr>
<td>beacon</td>
<td>enable</td>
<td>Sends beacons to advertise the SSID managed by the service profile.</td>
</tr>
<tr>
<td>cac-mode</td>
<td>none</td>
<td>Does not limit the number of active user sessions based on Call Admission Control (CAC).</td>
</tr>
<tr>
<td>cac-session</td>
<td>14</td>
<td>If session-based CAC is enabled (<a href="#">cac-mode</a> is set to <a href="#">session</a>), limits the number of active user sessions on a radio to 14.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default Value</td>
<td>Radio Behavior When Parameter Set to Default Value</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>cipher-ccmp</td>
<td>disable</td>
<td>Does not use Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to encrypt traffic sent to WPA clients.</td>
</tr>
<tr>
<td>cipher-tkip</td>
<td>enable</td>
<td>When the WPA IE is enabled, uses Temporal Key Integrity Protocol (TKIP) to encrypt traffic sent to WPA clients.</td>
</tr>
<tr>
<td>cipher-wep104</td>
<td>disable</td>
<td>Does not use Wired Equivalent Privacy (WEP) with 104-bit keys to encrypt traffic sent to WPA clients.</td>
</tr>
<tr>
<td>cipher-wep40</td>
<td>disable</td>
<td>Does not use WEP with 40-bit keys to encrypt traffic sent to WPA clients.</td>
</tr>
<tr>
<td>cos</td>
<td>0</td>
<td>If static CoS is enabled (static-cos is set to enable), assigns CoS 0 to all data traffic to or from clients.</td>
</tr>
<tr>
<td>dhcp-restrict</td>
<td>disable</td>
<td>Does not restrict a client’s traffic to only DHCP traffic while the client is being authenticated and authorized.</td>
</tr>
<tr>
<td>idle-client-probing</td>
<td>enable</td>
<td>Sends a keepalive packet (a null-data frame) to each client every 10 seconds.</td>
</tr>
<tr>
<td>long-retry-count</td>
<td>5</td>
<td>Sends a long unicast frame up to five times without acknowledgment.</td>
</tr>
<tr>
<td>no-broadcast</td>
<td>disable</td>
<td>Does not reduce wireless broadcast traffic by sending unicasts to clients for ARP requests, DHCP Offers, and Acks instead of forwarding them as multicasts.</td>
</tr>
<tr>
<td>proxy-arp</td>
<td>disable</td>
<td>Does not reply on behalf of wireless clients to ARP requests for client IP addresses. Instead, the radio forwards the ARP Requests as wireless broadcasts.</td>
</tr>
<tr>
<td>psk-phrase</td>
<td>No passphrase defined</td>
<td>Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.</td>
</tr>
<tr>
<td>psk-raw</td>
<td>No preshared key defined</td>
<td>Uses dynamically generated keys rather than statically configured keys to authenticate WPA clients.</td>
</tr>
<tr>
<td>rsn-ie</td>
<td>disable</td>
<td>Does not use the RSN IE in transmitted frames.</td>
</tr>
</tbody>
</table>
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

Table 74  Defaults for Service Profile Parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Radio Behavior When Parameter Set to Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>shared-key-auth</td>
<td>disable</td>
<td>Does not use shared-key authentication. This parameter does not enable PSK authentication for WPA. To enable PSK encryption for WPA, use the set radio-profile auth-psk command.</td>
</tr>
<tr>
<td>short-retry-count</td>
<td>5</td>
<td>Sends a short unicast frame up to five times without acknowledgment.</td>
</tr>
<tr>
<td>soda</td>
<td>disable</td>
<td>Sygate On Demand Agent (SODA) files are not downloaded to connecting clients.</td>
</tr>
<tr>
<td>ssid-name</td>
<td>private</td>
<td>Uses the SSID name <strong>private</strong>.</td>
</tr>
<tr>
<td>ssid-type</td>
<td>crypto</td>
<td>Encrypts wireless traffic for the SSID.</td>
</tr>
<tr>
<td>static-cos</td>
<td>disable</td>
<td>Assigns CoS based on the QoS mode (<strong>wmm</strong> or <strong>svp</strong>) or based on ACLs.</td>
</tr>
<tr>
<td>tkip-mc-time</td>
<td>60000</td>
<td>Uses Michael countermeasures for 60,000 ms (60 seconds) following detection of a second MIC failure within 60 seconds.</td>
</tr>
</tbody>
</table>
The table below shows the defaults for Service Profile Parameters (continued).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Radio Behavior When Parameter Set to Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmit-rates</td>
<td>802.11a:</td>
<td>Accepts associations only from clients that support one of the mandatory rates.</td>
</tr>
<tr>
<td></td>
<td>mandatory:</td>
<td>Sends beacons at the specified rate (6 Mbps for 802.11a, 2 Mbps for 802.11b/g).</td>
</tr>
<tr>
<td></td>
<td>6.0,12.0,24.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>beacon-rate:</td>
<td>Sends multicast data at the highest rate that can reach all clients connected to the radio.</td>
</tr>
<tr>
<td></td>
<td>6.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multicast-rate:</td>
<td>Accepts frames from clients at all valid data rates. (No rates are disabled by default.)</td>
</tr>
<tr>
<td></td>
<td>auto</td>
<td></td>
</tr>
<tr>
<td></td>
<td>disabled: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>802.11b:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mandatory:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.0,2.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>beacon-rate:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multicast-rate:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>auto</td>
<td></td>
</tr>
<tr>
<td></td>
<td>disabled: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>802.11g:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>mandatory:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.0,2.0,5.5,11.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>beacon-rate:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multicast-rate:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>auto</td>
<td></td>
</tr>
<tr>
<td></td>
<td>disabled: none</td>
<td></td>
</tr>
<tr>
<td>user-idle-timeout</td>
<td>180</td>
<td>Allows a client to remain idle for 180 seconds (3 minutes) before MSS changes the client’s session to the Disassociated state.</td>
</tr>
<tr>
<td>web-aaa-form</td>
<td>Not configured</td>
<td>For WebAAA users, serves the default login web page or, if configured, the SSID-specific login web page.</td>
</tr>
<tr>
<td>web-portal-session-timeout</td>
<td>5</td>
<td>Allows a Web Portal WebAAA session to remain in the Deassociated state 5 seconds before being terminated automatically.</td>
</tr>
</tbody>
</table>
Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You must configure the service profile before you can map it to a radio profile. You can map the same service profile to more than one radio profile.

You must disable all radios that use a radio profile before you can change parameters in the profile. Use the set radio-profile mode command.

Examples — The following command maps service-profile wpa_clients to radio profile rp2:

```
WX4400# set radio-profile rp2 service-profile wpa_clients
```

See Also
- display radio-profile on page 398
- display service-profile on page 401
- set service-profile attr on page 479
- set service-profile auth-dot1x on page 481
- set service-profile auth-fallthru on page 482
- set service-profile auth-psk on page 483
- set service-profile beacon on page 484
- set service-profile cac-mode on page 486
- set service-profile cac-session on page 487
- set service-profile cipher-ccmp on page 488
- set service-profile cipher-tkip on page 489
- set service-profile cipher-wep104 on page 490
- set service-profile cipher-wep40 on page 491
- set service-profile cos on page 492
- set service-profile dhcp-restrict on page 493
- set service-profile idle-client-probing on page 494
- set service-profile long-retry-count on page 497
- set service-profile no-broadcast on page 499
- set service-profile proxy-arp on page 500
- set service-profile psk-phrase on page 501
- set service-profile psk-raw on page 502
- set service-profile rsn-ie on page 503
- set service-profile shared-key-auth on page 504
- set service-profile short-retry-count on page 504
- set service-profile soda mode on page 510
- set service-profile ssid-name on page 513
- set service-profile ssid-type on page 514
- set service-profile static-cos on page 515
- set service-profile tkip-mc-time on page 514
- set service-profile transmit-rates on page 516
- set service-profile user-idle-timeout on page 519
- set service-profile web-portal-form on page 521
- set service-profile web-portal-session-timeout on page 525
- set service-profile wep active-multicast-index on page 526
- set service-profile wep active-unicast-index on page 527
- set service-profile wep key-index on page 528
- set service-profile wpa-ie on page 529
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set radio-profile short-retry</td>
<td>Deprecated in MSS Version 4.2. In 4.2, this parameter is associated with service profiles instead of radio profiles. See set service-profile short-retry-count on page 504.</td>
</tr>
<tr>
<td>set radio-profile wmm</td>
<td>Deprecated in MSS Version 4.2. To enable or disable WMM, see set radio-profile qos-mode on page 468.</td>
</tr>
<tr>
<td>set radio-profile wmm-powersave</td>
<td>Enables Unscheduled Automatic Powersave Delivery (U-APSD) on MAP radios managed by the radio profile. U-APSD enables WMM clients that use powersave mode to more efficiently request buffered unicast packets from MAP radios.</td>
</tr>
</tbody>
</table>

When U-APSD is enabled, a client can retrieve buffered unicast packets for a traffic priority enabled for U-APSD by sending a QoS data or QoS-Null frame for that priority. U-APSD can be enabled for individual traffic priorities, for individual clients, based on the client’s request. A client enables U-APSD for a traffic priority by indicating this preference when (re)associating with the MAP radio.

A client can but is not required to request U-APSD for all four traffic priorities. The MAP radio still buffers packets for all traffic priorities even if the client does not request U-APSD for them. However, to retrieve buffered packets for priorities that are not using U-APSD, a client must send a separate PSpoll for each buffered packet.

**Syntax** — set radio-profile name wmm-powersave {enable | disable}

- *name* — Radio profile name.
- *enable* — Enable U-APSD.
- *disable* — Disables U-APSD.

**Defaults** — U-APSD is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS 5.0.
Usage — U-APSD is supported only for QoS mode WMM. If WMM is not enabled on the radio profile, use the set radio-profile qos-mode command to enable it.

Examples — The following command enables U-APSD on radio profile rp1:

```
WX2200# set radio-profile rp1 wmm-powersave enable
success: change accepted.
```

See Also

- `set radio-profile mode` on page 464
- `set radio-profile qos-mode` on page 468
- `display radio-profile` on page 398

---

**set service-profile attr**

Configures authorization attributes that are applied by default to users accessing the SSID managed by the service profile. These SSID default attributes are applied in addition to any supplied by the RADIUS server or from the local database.

**Syntax** — `set service-profile name attr attribute-name value`

- **name** — Service profile name.
- **attribute-name value** — Name and value of an attribute you are using to authorize SSID users for a particular service or session characteristic. For a list of authorization attributes and values that you can assign to network users, see Table 45 on page 310. All of the attributes listed in Table 45 can be used with this command except ssid.

**Defaults** — By default, a service profile does not have any authorization attributes set.

**Access** — Enabled.

**History** — Introduced in MSS 4.1.

**Usage** — To change the value of a default attribute for a service profile, use the set `service-profile attr` command and specify a new value.
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

The SSID default attributes are applied in addition to any attributes supplied for the user by the RADIUS server or the local database. When the same attribute is specified both as an SSID default attribute and through AAA, then the attribute supplied by the RADIUS server or the local database takes precedence over the SSID default attribute. If a location policy is configured, the location policy rules also take precedence over SSID default attributes. The SSID default attributes serve as a fallback when neither the AAA process, nor a location policy, provides them.

For example, a service profile might be configured with the `service-type` attribute set to 2. If a user accessing the SSID is authenticated by a RADIUS server, and the RADIUS server returns the `vlan-name` attribute set to `orange`, then that user will have a total of two attributes set: `service-type` and `vlan-name`.

If the service profile is configured with the `vlan-name` attribute set to `blue`, and the RADIUS server returns the `vlan-name` attribute set to `orange`, then the attribute from the RADIUS server takes precedence; the user is placed in the orange VLAN.

You can display the attributes for each connected user and whether they are set through AAA or through SSID defaults by entering the `display sessions network verbose` command. You can display the configured SSID defaults by entering the `display service-profile` command.

**Examples** — The following command assigns users accessing the SSID managed by service profile `sp2` to VLAN `blue`:

```
WX4400# set service-prof sp2 attr vlan-name blue
success: change accepted.
```

The following command assigns users accessing the SSID managed by service profile `sp2` to the Mobility Profile `tulip`.

```
WX4400# set service-prof sp2 attr mobility-profile tulip
success: change accepted.
```

The following command limits the days and times when users accessing the SSID managed by service profile `sp2` can access the network, to 5 p.m. to 2 a.m. every weekday, and all day Saturday and Sunday:

```
WX1200# set service-prof sp2 attr time-of-day
Wk1700-0200,Sa,Su
success: change accepted.
```
set service-profile auth-dot1x

Disables or reenables 802.1X authentication of Wi-Fi Protected Access (WPA) clients by MAP radios, when the WPA information element (IE) is enabled in the service profile that is mapped to the radio profile that the radios are using.

**Syntax** — set service-profile

```plaintext
name auth-dot1x {enable | disable}
```

- **name** — Service profile name.
- **enable** — Enables 802.1X authentication of WPA clients.
- **disable** — Disables 802.1X authentication of WPA clients.

**Defaults** — When the WPA IE is enabled, 802.1X authentication of WPA clients is enabled by default. If the WPA IE is disabled, the `auth-dot1x` setting has no effect.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command does not disable dynamic WEP for non-WPA clients. To disable dynamic WEP for non-WPA clients, enable the WPA IE (if not already enabled) and disable the 40-bit WEP and 104-bit WEP cipher suites in the WPA IE, if they are not already disabled.

To use 802.1X authentication for WPA clients, you also must enable the WPA IE.

If you disable 802.1X authentication of WPA clients, the only method available for authenticating the clients is preshared key (PSK) authentication. To use this, you must enable PSK support and configure a passphrase or key.

**Examples** — The following command disables 802.1X authentication for WPA clients that use service profile `wpa_clients`:

```plaintext
WX4400# set service-profile wpa_clients auth-dot1x disable
success: change accepted.
```
See Also
- display service-profile on page 401
- set service-profile auth-psk on page 483
- set service-profile psk-phrase on page 501
- set service-profile wpa-ie on page 529

**set service-profile auth-fallthru**

Specifies the authentication type for users who do not match an 802.1X or MAC authentication rule for an SSID managed by the service profile. When a user tries to associate with an SSID, MSS checks the authentication rules for that SSID for a userglob that matches the username. If the SSID does not have an authentication rule that matches the username, authentication for the user falls through to the fallthru method.

The fallthru method is a service profile parameter, and applies to all radios within the radio profiles that are mapped to the service profile.

**Syntax** — set service-profile name auth-fallthru
{last-resort | none | web-portal}

- last-resort — Automatically authenticates the user and allows access to the SSID requested by the user, without requiring a username and password.
- none — Denies authentication and prohibits the user from accessing the SSID.

The fallthru authentication type none is different from the authentication method none you can specify for administrative access. The fallthru authentication type none denies access to a network user. In contrast, the authentication method none allows access to the WX switch by an administrator. (See “set authentication admin” on page 287 and “set authentication console” on page 289.)

- web-portal — Serves the user a web page from the WX switch’s nonvolatile storage for secure login to the network.

**Defaults** — The default fallthru authentication type is web-auth.

If a username does not match a userglob in an authentication rule for the SSID requested by the user, the WX switch that is managing the radio the user is connected to redirects the user to a web page located on the WX switch. The user must type a valid username and password on the web page to access the SSID.
set service-profile auth-psk

Access — Enabled.


Usage — The last-resort falthru authentication type allows any user to access any SSID managed by the service profile. This method does not require the user to provide a username or password. Use the last-resort method only if none of the SSIDs managed by the service profile require secure access.

The web-auth authentication type requires additional configuration items. (See the “Configuring AAA for Network Users” chapter of the Wireless LAN Switch and Controller Configuration Guide.)

Examples — The following command sets the falthru authentication for SSIDS managed by the service profile rnd_lab to none:

WX4400# set service-profile rnd_lab auth-fallthru none
success: change accepted.

See Also
- display service-profile on page 401
- set web-portal on page 326
- set service-profile web-portal-form on page 521

set service-profile auth-psk

Enables pre-shared key (PSK) authentication of Wi-Fi Protected Access (WPA) clients by MAP radios in a radio profile, when the WPA information element (IE) is enabled in the service profile.

Syntax — set service-profile name auth-psk {enable | disable}

- name — Service profile name.
- enable — Enables PSK authentication of WPA clients.
- disable — Disables PSK authentication of WPA clients.

Defaults — When the WPA IE is enabled, PSK authentication of WPA clients is enabled by default. If the WPA IE is disabled, the auth-psk setting has no effect.
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command affects authentication of WPA clients only.

To use PSK authentication, you also must configure a passphrase or key.
In addition, you must enable the WPA IE.

The WebAAA falthru authentication type is not supported in conjunction
with WPA encryption using preshared keys (PSK) for the same SSID. These
options are configurable together but are not compatible. WebAAA
traffic is not encrypted, whereas the PSK four-way handshake requires a
client to already be authenticated and for encryption to be in place.

Examples — The following command enables PSK authentication for
service profile wpa_clients:

WX4400# set service-profile wpa_clients auth-psk enable
success: change accepted.

See Also
- display service-profile on page 401
- set service-profile auth-dot1x on page 481
- set service-profile psk-raw on page 502
- set service-profile wpa-ie on page 529

set service-profile beacon

Disables or reenables beaconing of the SSID managed by the service
profile.

A MAP radio responds to an 802.11 probe any request with only the
beaconed SSID(s). For a nonbeaconed SSID, radios respond only to
directed 802.11 probe requests that match the nonbeaconed SSID’s SSID
string.

When you disable beaconing for an SSID, the radio still sends beacon
frames, but the SSID name in the frames is blank.

Syntax — set service-profile name beacon {enable | disable}
- name — Service profile name.
set service-profile bridging

Enables wireless bridging for a service profile configured for WLAN mesh services.

**Syntax** — `set service-profile mesh-service-profile bridging {enable | disable}`

- `mesh-service-profile` — Mesh service profile name.
- `enable` — Enables wireless bridging for the service profile.
- `disable` — Disables wireless bridging for the service profile.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.
**Usage** — WLAN mesh services can be used in a wireless bridge configuration, implementing MAPs as bridge endpoints in a transparent Layer 2 bridge. A typical application of wireless bridging is to provide network connectivity between two buildings using a wireless link.

A Mesh Portal AP serving as a bridge endpoint can support up to five Mesh APs serving as bridge endpoints. A Mesh AP serving as a bridge endpoint picks up packets from its wired port and transfers them to the other bridge endpoint. A simple source/destination learning mechanism is used in order to avoid forwarding packets across the bridge unnecessarily.

When wireless bridging is enabled for a service profile, the MAPs with the applied service profile serve as bridge peers. When a Mesh AP associates with a Mesh Portal AP through this service profile, the Mesh Portal AP automatically configures the Mesh AP to operate in bridge mode.

**Examples** — The following command enables wireless bridging on service profile *sp1*:

```
WX# set service-profile sp1 bridging enable
success: change accepted.
```

**See Also**
- `display ap mesh-links` on page 377
- `set ap boot-configuration mesh ssid` on page 421
- `set service-profile mesh` on page 498

### set service-profile cac-mode

Configures the Call Admission Control (CAC) mode.

**Syntax** — `set service-profile name cac-mode {none | session}`

- `name` — Service profile name.
- `none` — CAC is not used.
- `session` — CAC is based on the number of active sessions.

**Defaults** — The default CAC mode is `none`.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.
Examples — The following command enables session-based CAC on service profile sp1:

WX4400# set service-profile sp1 cac-mode session
success: change accepted.

See Also
- display service-profile on page 401
- set service-profile cac-session on page 487

```
set service-profile cac-session
```

Specifies the maximum number of active sessions a radio can have when session-based CAC is enabled. When a MAP radio has reached the maximum allowed number of active sessions, the radio refuses connections from additional clients.

Syntax — set service-profile name cac-session max-sessions

- name — Service profile name.
- max-sessions — Maximum number of active sessions allowed on the radio.

Defaults — The default number of sessions allowed is 14.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — This command applies only when the CAC mode is session. If the CAC mode is none, you can still change the maximum number of sessions, but the setting does not take effect until you change the CAC mode to session. To change the CAC mode, use the set service-profile cac-mode command.

Examples — The following command changes the maximum number of sessions for radios used by service profile sp1 to 10:

WX4400# set service-profile sp1 cac-session 10
success: change accepted.

See Also
- display service-profile on page 401
- set service-profile cac-mode on page 486
set service-profile cipher-ccmp

Enables Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encryption with WPA clients, for a service profile.

**Syntax** — set service-profile name cipher-ccmp {enable | disable}

- name — Service profile name.
- enable — Enables CCMP encryption for WPA clients.
- disable — Disables CCMP encryption for WPA clients.

**Defaults** — CCMP encryption is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To use CCMP, you must also enable the WPA IE.

**Examples** — The following command configures service profile sp2 to use CCMP encryption:

WX4400# set service-profile sp2 cipher-ccmp enable
success: change accepted.

**See Also**

- display service-profile on page 401
- set service-profile cipher-tkip on page 489
- set service-profile cipher-wep104 on page 490
- set service-profile cipher-wep40 on page 491
- set service-profile wpa-ie on page 529
**set service-profile cipher-tkip**

Disables or reenables Temporal Key Integrity Protocol (TKIP) encryption in a service profile.

**Syntax** — set service-profile

```plaintext
name cipher-tkip {enable | disable}
```

- `name` — Service profile name.
- `enable` — Enables TKIP encryption for WPA clients.
- `disable` — Disables TKIP encryption for WPA clients.

**Defaults** — When the WPA IE is enabled, TKIP encryption is enabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To use TKIP, you must also enable the WPA IE.

**Examples** — The following command disables TKIP encryption in service profile `sp2`:

```plaintext
WX4400# set service-profile sp2 cipher-tkip disable
success: change accepted.
```

**See Also**

- `display service-profile` on page 401
- `set service-profile cipher-ccmp` on page 488
- `set service-profile cipher-wep104` on page 490
- `set service-profile cipher-wep40` on page 491
- `set service-profile tkip-mc-time` on page 514
- `set service-profile wpa-ie` on page 529
set service-profile cipher-wep104

Enables dynamic Wired Equivalent Privacy (WEP) with 104-bit keys, in a service profile.

Syntax — set service-profile name cipher-wep104 {enable | disable}

- name — Service profile name.
- enable — Enables 104-bit WEP encryption for WPA clients.
- disable — Disables 104-bit WEP encryption for WPA clients.

Defaults — 104-bit WEP encryption is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To use 104-bit WEP with WPA clients, you must also enable the WPA IE.

When 104-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 40-bit dynamic WEP, you must enable WEP with 40-bit keys. Use the set service-profile cipher-wep40 command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the set service-profile wep commands.

To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the set service-profile wep key-index command.

Examples — The following command configures service profile sp2 to use 104-bit WEP encryption:

WX4400# set service-profile sp2 cipher-wep104 enable
success: change accepted.
set service-profile cipher-wep40

Enables dynamic Wired Equivalent Privacy (WEP) with 40-bit keys, in a service profile.

**Syntax** — set service-profile **name** cipher-wep40 **{enable | disable}**

- **name** — Service profile name.
- **enable** — Enables 40-bit WEP encryption for WPA clients.
- **disable** — Disables 40-bit WEP encryption for WPA clients.

**Defaults** — 40-bit WEP encryption is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To use 40-bit WEP with WPA clients, you must also enable the WPA IE.

When 40-bit WEP in WPA is enabled in the service profile, radios managed by a radio profile that is mapped to the service profile can also support non-WPA clients that use dynamic WEP.

To support WPA clients that use 104-bit dynamic WEP, you must enable WEP with 104-bit keys in the service profile. Use the **set service-profile cipher-wep104** command.

Microsoft Windows XP does not support WEP with WPA. To configure a service profile to provide dynamic WEP for XP clients, leave WPA disabled and use the **set service-profile wep** commands.
To support non-WPA clients that use static WEP, you must configure static WEP keys. Use the `set service-profile wep key-index` command.

**Examples** — The following command configures service profile `sp2` to use 40-bit WEP encryption:

```
WX4400# set service-profile sp2 cipher-wep40 enable
success: change accepted.
```

**See Also**

- display service-profile on page 401
- set service-profile cipher-ccmp on page 488
- set service-profile cipher-tkip on page 489
- set service-profile cipher-wep104 on page 490
- set service-profile wep key-index on page 528
- set service-profile wpa-ie on page 529

---

**set service-profile cos**

Sets the Class-of-Service (CoS) level for static CoS.

**Syntax** — `set service-profile name cos level`

- `name` — Service profile name.
- `level` — CoS value assigned by the MAP to all traffic in the service profile.

**Defaults** — The default static CoS level is 0.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — This command applies only when static CoS is enabled. If static CoS is disabled, prioritization is based on the QoS mode configured in the radio profile, and on any ACLs that set CoS. (See the “Configuring Quality of Service” chapter of the *Wireless LAN Switch and Controller Configuration Guide.*) To enable static CoS, use the `set service-profile static-cos` command.

**Examples** — The following command changes the static CoS level to 7 (voice priority):

```
WX4400# set service-profile sp2 cos 7
success: change accepted.
```
set service-profile dhcp-restrict

Enables or disables DHCP Restrict on a service profile. DHCP Restrict filters the traffic from a newly associated client and allows DHCP traffic only, until the client has been authenticated and authorized. All other traffic is captured by the WX and is not forwarded. After the client is successfully authorized, the traffic restriction is removed.

**Syntax** — `set service-profile name dhcp-restrict {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables DHCP Restrict.
- **disable** — Disables DHCP Restrict.

**Examples** — DHCP Restrict is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — To further reduce the overhead of DHCP traffic, use the `set service-profile no-broadcast` command to disable DHCP broadcast traffic from MAP radios to clients on the service profile's SSID.

**Examples** — The following command enables DHCP Restrict on service profile sp1:

```
WX4400# set service-profile sp1 dhcp-restrict enable
success: change accepted.
```

**See Also**

- `display service-profile` on page 401
- `set service-profile static-cos` on page 515

---

WX4400# set service-profile sp1 cos 7
success: change accepted.

**See Also**

- `display service-profile` on page 401
- `set service-profile static-cos` on page 515
Disables or reenables periodic keepalives from MAP radios to clients on a service profile's SSID. When idle-client probing is enabled, the MAP radio sends a unicast null-data frame to each client every 10 seconds. Normally, a client that is still active sends an Ack in reply to the keepalive.

If a client does not send any data or respond to any keepalives before the user idle timeout expires, MSS changes the client session to the Disassociated state.

**Syntax** — set service-profile name idle-client-probing

- `enable` — Enables keepalives.
- `disable` — Disables keepalives.

**Defaults** — Idle-client probing is enabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — The length of time a client can remain idle (unresponsive to idle-client probes) is specified by the user-idle-timeout command.

**Examples** — The following command disables idle-client keepalives on service profile `sp1`:

```
WX4400# set service-profile sp1 idle-client-probing disable
success: change accepted.
```

**See Also**

- `display service-profile` on page 401
- `set service-profile user-idle-timeout` on page 519
set service-profile keep-initial-vlan

Configures MAP radios managed by the radio profile to leave a roamed user on the VLAN assigned by the switch where the user logged on. When this option is disabled, a user’s VLAN is reassigned by each WX switch to which a user roams.

**Syntax**

`set service-profile name keep-initial-vlan {enable | disable}`

- `name` — Service profile name.
- `enable` — Enables radios to leave a roamed user on the same VLAN instead of reassigning the VLAN.
- `disable` — Configures radios to reassign a roamed user’s VLAN.

**Defaults** — This option is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 5.0.

**Usage** — Even when this option is enabled, the WX switch to which a user roams (the roamed-to switch) can reassign the VLAN in any of the following cases:

- A location policy on the local switch reassigns the VLAN.
- The user is configured in the switch’s local database and the VLAN-Name attribute is set on the user or on a user group the user is in.
- The access rule on the roamed-to switch uses RADIUS, and the VLAN-Name attribute is set on the RADIUS server.

**Examples** — The following command enables the `keep-initial-vlan` option on service profile `sp3`:

```
WX1200# set service-profile sp3 keep-initial-vlan enable
success: change accepted.
```

**See Also**

- `display service-profile` on page 401
### set service-profile load-balancing-exempt

Exempts a service profile from performing RF load balancing.

**Syntax**
```
set service-profile name load-balancing-exempt {enable | disable}
```
- **name** — Service profile name.
- **enable** — Exempts the specified service profile from RF load balancing.
- **disable** — If a service profile has previously been exempted from RF load balancing, restores RF load balancing for the service profile.

**Defaults** — By default, MAP radios automatically perform RF load balancing for all service profiles.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — Use this command to exempt a service profile from RF load balancing. Exempting a service profile from RF load balancing means that even if an MAP radio is attempting to steer clients away, it does not reduce or conceal the availability of the SSID named in the exempted service profile. Even if a radio is withholding probe responses to manage its load, the radio does respond to probes for an exempt SSID. Also, if an MAP radio is withholding probe responses, and a client probes for any SSID, and the radio has at least one exempt SSID, the radio responds to the probe, but the response reveals only the exempt SSID(s).

**Examples** — The following command exempts service profile `sp3` from RF load balancing:

```
WX# set service-profile sp3 load-balancing-exempt enable
success: change accepted.
```

**See Also**
- `display load-balancing group` on page 396
- `set load-balancing strictness` on page 447
- `set ap radio load balancing` on page 437
- `set ap local-switching mode` on page 427
Changes the long retry threshold for a service profile. The long retry threshold specifies the number of times a radio can send a long unicast frame without receiving an acknowledgment. A long unicast frame is a frame that is equal to or longer than the frag-threshold.

**Syntax** — `set service-profile name long-retry-count threshold`

- **name** — Service profile name.
- **threshold** — Number of times the radio can send the same long unicast frame. You can enter a value from 1 through 15.

**Defaults** — The default long unicast retry threshold is 5 attempts.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Examples** — The following command changes the long retry threshold for service profile `sp1` to 8:

```
WX4400# set service-profile sp1 long-retry-count 8
success: change accepted.
```

**See Also**

- `set radio-profile frag-threshold` on page 461
- `set service-profile short-retry-count` on page 504
- `display service-profile` on page 401
set service-profile mesh

Creates a service profile for use with WLAN mesh services.

**Syntax** — `set service-profile name mesh mode {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables mesh services for the service profile.
- **disable** — Disables mesh services for the service profile.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.

**Usage** — Use this command to configure mesh services for a service profile. Once configured, the service profile can then be mapped to a radio profile that manages a radio on the Mesh Portal MAP, which then allows a Mesh Portal AP to beacon a mesh services SSID to Mesh APs.

**Examples** — The following command enables mesh services for service profile `sp1`:

```
WX# set service-profile sp1 mesh mode enable
success: change accepted.
```

**See Also**
- `display ap mesh-links` on page 377
- `set ap boot-configuration mesh ssid` on page 421
Disables or reenables the no-broadcast mode. The no-broadcast mode helps reduce traffic overhead on an SSID by having more SSID bandwidth available for unicast traffic. The no-broadcast mode also helps VoIP handsets conserve power by reducing the amount of broadcast traffic sent to the phones.

When enabled, the no-broadcast mode prevents MAP radios from sending DHCP or ARP broadcasts to clients on the service profile’s SSID. Instead, a MAP radio handles this traffic as follows:

- **ARP requests**—If the SSID has clients with IP addresses that the WX does not already know, the WX allows the MAP radio to send the ARP request as a unicast to only those stations whose addresses the WX does not know. The MAP radio does not forward the ARP request as a broadcast and does not send the request as a unicast to stations whose addresses the WX already knows.

- **DHCP Offers or Acks**—If the destination MAC address belongs to a client on the SSID, the MAP radio sends the DHCP Offer or Ack as a unicast to that client only.

The no-broadcast mode does not affect other types of broadcast traffic and does not prevent clients from sending broadcasts.

**Syntax** — `set service-profile name no-broadcast {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables the no-broadcast mode. MAP radios are not allowed to send broadcast traffic to clients on the service profile’s SSID.
- **disable** — Disables the no-broadcast mode.

**Defaults** — The no-broadcast mode is disabled by default. (Broadcast traffic not disabled.)

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — To further reduce ARP traffic on a service profile, use the `set service-profile proxy-arp` command to enable Proxy ARP.
Examples — The following command enables the no-broadcast mode on service profile sp1:

WX4400# set service-profile sp1 no-broadcast enable
success: change accepted.

See Also
- display service-profile on page 401
- set service-profile dhcp-restrict on page 493
- set service-profile proxy-arp on page 500

set service-profile proxy-arp

Enables proxy ARP. When proxy ARP is enabled, the WX replies to ARP requests for client IP address on behalf of the clients. This feature reduces broadcast overhead on a service profile SSID by eliminating ARP broadcasts from MAP radios to the SSID’s clients.

If the ARP request is for a client with an IP address the WX does not already know, the WX allows MAP radios to send the ARP request to clients. If the no-broadcast mode is also enabled, the MAP radios send the ARP request as a unicast to only the clients whose addresses the WX does not know. However, if no-broadcast mode is disabled, the MAP radios sends the ARP request as a broadcast to all clients on the SSID.

Syntax — set service-profile name proxy-arp {enable | disable}

- name — Service profile name.
- enable — Enables proxy ARP.
- disable — Disables proxy ARP.

Defaults — Proxy ARP is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — To further reduce broadcast traffic on a service profile, use the set service-profile no-broadcast command to disable DHCP and ARP request broadcasts.
Examples — The following command enables proxy ARP on service profile sp1:

WX4400# set service-profile sp1 proxy-arp enable
success: change accepted.

See Also

- display service-profile on page 401
- set service-profile dhcp-restrict on page 493
- set service-profile no-broadcast on page 499

---

**set service-profile psk-phrase**

Configures a passphrase for preshared key (PSK) authentication to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

**Syntax** — 

```
set service-profile name psk-phrase passphrase
```

- `name` — Service profile name.
- `passphrase` — An ASCII string from 8 to 63 characters long. The string can contain blanks if you use quotation marks at the beginning and end of the string.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — MSS converts the passphrase into a 256-bit binary number for system use and a raw hexadecimal key to store in the WX configuration. Neither the binary number nor the passphrase itself is ever displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable the WPA IE.
Examples — The following command configures service profile sp3 to use passphrase "1234567890123<>?+=&% The quick brown fox jumps over the lazy sl":

WX4400# set service-profile sp3 psk-phrase "1234567890123<>?+=&% The quick brown fox jumps over the lazy sl"

success: change accepted.

See Also
- display service-profile on page 401
- set mac-user attr on page 309
- set service-profile auth-psk on page 483
- set service-profile psk-raw on page 502
- set service-profile wpa-ie on page 529

set service-profile psk-raw
Configures a raw hexadecimal preshared key (PSK) to use for authenticating WPA clients, in a service profile. Radios use the PSK as a pairwise master key (PMK) to derive unique pairwise session keys for individual WPA clients.

Syntax — set service-profile name psk-raw hex
- name — Service profile name.
- hex — A 64-bit ASCII string representing a 32-digit hexadecimal number. Enter the two-character ASCII form of each hexadecimal number.

Defaults — None.

Examples — Enabled.

History — Introduced in MSS Version 3.0.

Usage — MSS converts the hexadecimal number into a 256-bit binary number for system use. MSS also stores the hexadecimal key in the WX configuration. The binary number is never displayed in the configuration.

To use PSK authentication, you must enable it and you also must enable WPA IE.
**Examples** — The following command configures service profile sp3 to use a raw PSK with PSK clients:

```
WX4400# set service-profile sp3 psk-raw c25d3fe4483e867
d1df96eaacdf8b02451fa0836162e758100f5f6b87965e59d
success: change accepted.
```

**See Also**
- `display service-profile` on page 401
- `set mac-user attr` on page 309
- `set service-profile auth-psk` on page 483
- `set service-profile psk-phrase` on page 501
- `set service-profile wpa-ie` on page 529

---

**set service-profile rsn-ie**

Enables the Robust Security Network (RSN) Information Element (IE).

The RSN IE advertises the RSN authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

**Syntax** — `set service-profile name rsn-ie {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables the RSN IE.
- **disable** — Disables the RSN IE.

**Defaults** — The RSN IE is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command enables the RSN IE in service profile sprsn:

```
WX4400# set service-profile sprsn rsn-ie enable
success: change accepted.
```

**See Also**
- `display service-profile` on page 401
- `set service-profile cipher-ccmp` on page 488
set service-profile shared-key-auth

Enables shared-key authentication, in a service profile.

Use this command only if advised to do so by 3Com. This command does not enable preshared key (PSK) authentication for Wi-Fi Protected Access (WPA). To enable PSK encryption for WPA, use the set service-profile auth-psk command.

Syntax — set service-profile name shared-key-auth {enable | disable}

- **name** — Service profile name.
- **enable** — Enables shared-key authentication.
- **disable** — Disables shared-key authentication.

Defaults — Shared-key authentication is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command enables shared-key authentication in service profile sp4:

```
WX4400# set service-profile sp4 shared-key-auth enable
success: change accepted.
```

See Also —

- display radio-profile on page 398
- set radio-profile mode on page 464
- set service-profile cipher-tkip on page 489

set service-profile short-retry-count

Changes the short retry threshold for a service profile. The short retry threshold specifies the number of times a radio can send a short unicast frame without receiving an acknowledgment. A short unicast frame is a frame that is shorter than the frag-threshold.

Syntax — set service-profile name short-retry-count threshold

- **name** — Service profile name.
**set service-profile soda agent-directory**

Specifies the directory on the WX where the SODA agent files for a service profile are located.

**Syntax**

```
set service-profile name soda agent-directory directory
```

- **name** — Service profile name.
- **directory** — Directory on the WX for SODA agent files.

**Defaults** — By default, the WX expects SODA agent files to be located in a directory with the same name as SSID.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — If the same SODA agent is used for multiple service profiles, you can use this command to specify a single directory for SODA agent files on the WX, rather than placing the same SODA agent files in a separate directory for each service profile.

- **threshold** — Number of times a radio can send the same short unicast frame. You can enter a value from 1 through 15.

**Defaults** — The default short unicast retry threshold is 5 attempts.

**Examples** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Examples** — The following command changes the short retry threshold for service profile sp1 to 3:

```
WX4400# set service-profile sp1 short-retry-count 3
success: change accepted.
```

**See Also**

- [display service-profile](#) on page 401
- [set radio-profile frag-threshold](#) on page 461
- [set service-profile long-retry-count](#) on page 497
**Examples** — The following command specifies *soda-agent* as the location for SODA agent files for service profile *sp1*:

WX4400# set service-profile *sp1* soda agent-directory soda-agent
success: change accepted.

**See Also**

- display service-profile on page 401
- install soda agent on page 721
- uninstall soda agent on page 736

---

**set service-profile
c soda enforce-checks**

Specifies whether a client is allowed access to the network after it has downloaded and run the SODA agent security checks.

**Syntax** — `set service-profile name soda enforce-checks {enable | disable}

- **name** — Service profile name.
- **enable** — SODA agent checks are performed before the client is allowed access to the network.
- **disable** — Allows the client access to the network immediately after the SODA agent is downloaded, without waiting for the checks to be run.

**Defaults** — By default, SODA agent checks are performed before the client is allowed access to the network.

**Access** — Enabled

**History** — Introduced in MSS Version 4.2.

**Usage** — When the SODA agent is enabled in a service profile, by default the SODA agent checks are downloaded to a client and run before the client is allowed on the network. You can use this command to disable the enforcement of the SODA security checks, so that the client is allowed access to the network immediately after the SODA agent is downloaded, rather than waiting for the security checks to be run.
When the enforce checks option is enabled, upon successful completion of the SODA agent checks, the client performs an HTTP Get operation to load the success page. Upon loading the success page, the client is granted access to the network.

In order for the client to load the success page, you must make sure the SODA agent is configured (through SODA Manager) with the correct URL of the success page, so that the WX can serve the page to the client.

Similarly, you must make sure the SODA agent is configured with the correct URLs of the failure and logout pages, so that when the client requests these pages, the WX can serve those pages as well.

**Examples** — The following command allows network access to clients after they have downloaded the SODA agent, but without requiring that the SODA agent checks be completed:

```
WX4400# set service-profile sp1 soda enforce-checks disable
success: change accepted.
```

**See Also**

- display service-profile on page 401
- set service-profile soda mode on page 510

---

**set service-profile soda failure-page**

Specifies a page on the WX that loads when a client fails the security checks performed by the SODA agent.

**Syntax** — `set service-profile name soda failure-page page`

- `name` — Service profile name.
- `page` — Page that is loaded if the client fails the security checks performed by the SODA agent.

**Defaults** — By default, the WX dynamically generates a page indicating that the SODA agent checks have failed.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.
**Usage** — Use this command to specify a custom page to be loaded by the client when the SODA agent checks fail. After this page is loaded, the specified remediation ACL takes effect, or if there is no remediation ACL configured, then the client is disconnected from the network.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

The page is assumed to reside in the root directory on the WX. You can optionally specify a different directory where the page resides.

**Examples** — The following command specifies *failure.html* as the page to load when a client fails the SODA agent checks:

```
WX4400# set service-profile sp1 soda failure-page
    failure.html
success: change accepted.
```

The following command specifies *failure.html*, in the *soda-files* directory, as the page to load when a client fails the SODA agent checks:

```
WX4400# set service-profile sp1 soda failure-page
    soda-files/failure.html
success: change accepted.
```

**See Also**
- *display service-profile* on page 401
- *set service-profile soda enforce-checks* on page 506
- *set service-profile soda remediation-acl* on page 511

### set service-profile soda logout-page

Specifies a page on the WX that is loaded when a client logs out of the network by closing the SODA virtual desktop.

**Syntax** — `set service-profile name soda logout-page page`

- **name** — Service profile name.
- **page** — Page that is loaded when the client closes the SODA virtual desktop.

**Defaults** — None.

**Access** — Enabled.
**History** — Introduced in MSS Version 4.2.

**Usage** — When a client closes the SODA virtual desktop, the client is automatically disconnected from the network. You can use this command to specify a page that loads when the client closes the SODA virtual desktop.

The client can request this page at any time, to ensure that the client’s session has been terminated. You can add the IP address of the WX switch to the DNS server as a well-known name, and you can advertise the URL of the page to users as a logout page.

The page is assumed to reside in the root directory on the WX switch. You can optionally specify a different directory where the page resides.

For the logout page to load properly, you must enable the HTTPS server on the WX switch, so that clients can access the page using HTTPS. To do this, use the `set ip https server enable` command.

**Examples** — The following command specifies `logout.html` as the page to load when a client closes the SODA virtual desktop:

```
WX4400# set service-profile sp1 soda logout-page logout.html
success: change accepted.
```

The following command specifies `logout.html`, in the `soda-files` directory, as the page to load when a client closes the SODA virtual desktop:

```
WX4400# set service-profile sp1 soda logout-page soda-files/logout.html
success: change accepted.
```

**See Also**
- display service-profile on page 401
- set ip https server on page 225
**set service-profile soda mode**

Enables or disables Sygate On-Demand (SODA) functionality for a service profile.

**Syntax** — `set service-profile name soda mode {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables SODA functionality for the service profile.
- **disable** — Disables SODA functionality for the service profile.

**Defaults** — Disabled.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — When SODA functionality is enabled for a service profile, a SODA agent is downloaded to clients attempting to connect to a MAP managed by the service profile. The SODA agent performs a series of security-related checks on the client; if the client passes the checks, it can be admitted to the network.

In release 4.2, SODA functionality requires that Web Portal WebAAA also be enabled for the service profile.

**Examples** — The following command enables SODA functionality for service profile `sp1`:

```
WX4400# set service-profile sp1 soda mode enable
success: change accepted.
```

**See Also**

- `display service-profile` on page 401
- `install soda agent` on page 721
- `set service-profile soda enforce-checks` on page 506
set service-profile soda remediation-acl

Specifies an ACL to be applied to a client if it fails the checks performed by the SODA agent.

**Syntax** — `set service-profile name soda remediation-acl acl-name`

- **name** — Service profile name.
- **acl-name** — Name of an existing security ACL to use as a remediation ACL for this service profile. ACL names must start with a letter and are case-insensitive.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — If the SODA agent checks fail on a client, by default the client is disconnected from the network. Optionally, you can specify a *failure page* for the client to load (with the `set service-profile soda failure-page` command). When the failure page is loaded, you can optionally specify a *remediation ACL* to apply to the client. The remediation ACL can be used to grant the client limited access to network resources, for example. If there is no remediation ACL configured, then the client is disconnected from the network when the failure page is loaded.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

**Examples** — The following command configures the WX to apply `acl-1` to a client when it loads the failure page:

```
WX4400# set service-profile sp1 soda remediation-acl acl-1
success: change accepted.
```

**See Also**

- `display service-profile` on page 401
- `set service-profile soda enforce-checks` on page 506
- `set service-profile soda failure-page` on page 507
set service-profile soda success-page

Specifies a page on the WX that loads when a client passes the security checks performed by the SODA agent.

**Syntax** — `set service-profile name soda success-page page`

- **name** — Service profile name.
- **page** — Page that is loaded if the client passes the security checks performed by the SODA agent.

**Defaults** — By default, the WX switch generates a page indicating that the client passed the SODA agent checks.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — Use this command to specify a custom page loaded by the client when it passes the checks performed by the SODA agent. After this page is loaded, the client is placed in its assigned VLAN and granted access to the network.

The page is assumed to reside in the root directory on the WX. You can optionally specify a different directory where the page resides.

This functionality occurs only when the enforce checks option is enabled for the service profile. The enforce checks option is enabled by default.

**Examples** — The following command specifies `success.html`, which resides in the root directory on the WX, as the page to load when a client passes the SODA agent checks:

```
WX4400# set service-profile sp1 soda success-page success.html
success: change accepted.
```

The following command specifies `success.html`, which resides in the `soda-files` directory on the WX switch, as the page to load when a client passes the SODA agent checks:

```
WX4400# set service-profile sp1 soda success-page soda-files/success.html
success: change accepted.
```
See Also

- **display service-profile** on page 401
- **set service-profile soda enforce-checks** on page 506
- **set service-profile soda mode** on page 510

---

**set service-profile ssid-name**

Configures the SSID name in a service profile.

**Syntax** — `set service-profile name ssid-name ssid-name`  
- `name` — Service profile name.  
- `ssid-name` — Name of up to 32 alphanumeric characters. You can include blank spaces in the name, if you delimit the name with single or double quotation marks. You must use the same type of quotation mark (either single or double) on both ends of the string.

**Defaults** — The default SSID name is `private`.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Support added for blank spaces in the SSID name in MSS Version 4.0.

**Examples** — The following command applies the name `guest` to the SSID managed by service profile `clear_wlan`:

```
WX4400# set service-profile clear_wlan ssid-name guest  
success: change accepted.
```

See Also

- **display service-profile** on page 401
- **set service-profile ssid-type** on page 514
set service-profile ssid-type

Specifies whether the SSID managed by a service profile is encrypted or unencrypted.

**Syntax** — `set service-profile name ssid-type [clear | crypto]`

- `name` — Service profile name.
- `clear` — Wireless traffic for the service profile's SSID is not encrypted.
- `crypto` — Wireless traffic for the service profile's SSID is encrypted.

**Defaults** — The default SSID type is crypto.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command changes the SSID type for service profile `clear_wlan` to `clear`:

```
WX4400# set service-profile clear_wlan ssid-type clear
success: change accepted.
```

**See Also**

- `display service-profile` on page 401
- `set service-profile ssid-name` on page 513

---

set service-profile tkip-mc-time

Changes the length of time that MAP radios use countermeasures if two message integrity code (MIC) failures occur within 60 seconds. When countermeasures are in effect, MAP radios dissociate all TKIP and WPA WEP clients and refuse all association and reassociation requests until the countermeasures end.

**Syntax** — `set service-profile name tkip-mc-time wait-time`

- `name` — Service profile name.
- `wait-time` — Number of milliseconds (ms) countermeasures remain in effect. You can specify from 0 to 60,000.

**Defaults** — The default countermeasures wait time is 60,000 ms (60 seconds).

**Access** — Enabled.
set service-profile static-cos

**History** — Introduced in MSS Version 3.0.

**Usage** — Countermeasures apply only to TKIP and WEP clients. This includes WPA WEP clients and non-WPA WEP clients. CCMP clients are not affected.

The TKIP cipher suite must be enabled. The WPA IE also must be enabled.

**Examples** — The following command changes the countermeasures wait time for service profile sp3 to 30,000 ms (30 seconds):

```
WX4400# set service-profile sp3 tkip-mc-time 30000
success: change accepted.
```

**See Also**
- `display service-profile` on page 401
- `set service-profile cipher-tkip` on page 489
- `set service-profile wpa-ie` on page 529

---

**set service-profile static-cos**

Enables or disables static CoS on a service profile. Static CoS assigns the same CoS level to all traffic on the service profile's SSID, regardless of 802.1p or DSCP markings in the packets themselves, and regardless of any ACLs that mark CoS. This option provides a simple way to configure an SSID for priority traffic such as VoIP traffic.

When static CoS is enabled, the standard MSS prioritization mechanism is not used. Instead, the MAP sets CoS as follows:

- For traffic from the MAP to clients, the MAP places the traffic into the forwarding queue that corresponds to the CoS level configured on the service profile. For example, if the static CoS level is set to 7, the MAP radio places client traffic in its Voice queue.
- For traffic from clients to the network, the MAP marks the DSCP value in the IP headers of the tunnel packets used to carry the user data from the MAP to the WX switch.

**Syntax** — `set service-profile name static-cos {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables static CoS on the service profile.
- **disable** — Disables static CoS on the service profile.
Defaults — Static CoS is disabled by default.

Access — Enabled.

History — Introduced in MSS Version 4.2.

Usage — The CoS level is specified by the `set service-profile cos` command.

Examples — The following command enables static CoS on service profile `sp1`:

```
WX4400# set service-profile sp1 static-cos enable
success: change accepted.
```

See Also

- `display service-profile` on page 401
- `set service-profile cos` on page 492

---

**set service-profile transmit-rates** Changes the data rates supported by MAP radios for a service-profile SSID.

**Syntax** — `set service-profile name transmit-rates {11a | 11b | 11g} mandatory rate-list [disabled rate-list] [beacon-rate rate] [multicast-rate {rate | auto}]`

- `name` — Service profile name.
- `11a | 11b | 11g` — Radio type.
- `mandatory rate-list` — Set of data transmission rates that clients are required to support in order to associate with an SSID on a MAP radio. A client must support at least one of the mandatory rates.

These rates are advertised in the basic rate set of 802.11 beacons, probe responses, and reassociation response frames sent by MAP radios.

Data frames and management frames sent by MAP radios use one of the specified mandatory rates.
The valid rates depend on the radio type:

- **11a**—6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0
- **11b**—1.0, 2.0, 5.5, 11.0
- **11g**—1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, 54.0

Use a comma to separate multiple rates; for example: **6.0,9.0,12.0**

- **disabled rate-list** — Data transmission rates that MAP radios do not use to transmit data. This setting applies only to data sent by the MAP radios. The radios still accept frames from clients at disabled data rates.

The valid rates depend on the radio type and are the same as the valid rates for **mandatory**.

- **beacon-rate rate** — Data rate of beacon frames sent by MAP radios. This rate is also used for probe-response frames.

The valid rates depend on the radio type and are the same as the valid rates for **mandatory**. However, you cannot set the beacon rate to a disabled rate.

- **multicast-rate {rate | auto}** — Data rate of multicast frames sent by MAP radios.
  - **rate**—Sets the multicast rate to a specific rate. The valid rates depend on the radio type and are the same as the valid rates for **mandatory**. However, you cannot set the multicast rate to a disabled rate.
  - **auto**—Sets the multicast rate to the highest rate that can reach all clients connected to the MAP radio.

**Defaults** — This command has the following defaults:

- **mandatory**:
  - **11a**—6.0, 12.0, 24.0
  - **11b**—1.0, 2.0
  - **11g**—1.0, 2.0, 5.5, 11.0

- **disabled**—None. All rates applicable to the radio type are supported by default.
CHAPTER 11: MANAGED ACCESS POINT COMMANDS

- **beacon-rate:**
  - 11a—6.0
  - 11b—2.0
  - 11g—2.0
- **multicast-rate**—**auto** for all radio types.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — If you disable a rate, you cannot use the rate as a mandatory rate or the beacon or multicast rate. All rates that are applicable to the radio type and that are not disabled are supported by the radio.

**Examples** — The following command sets 802.11a mandatory rates for service profile sp1 to 6 Mbps and 9 Mbps, disables rates 48 Mbps and 54 Mbps, and changes the beacon rate to 9 Mbps:

```
WX4400# set service-profile sp1 transmit-rates 11a mandatory 6.0,9.0 disabled 48.0,54.0 beacon-rate 9.0
success: change accepted.
```

**See Also**
- **display service-profile** on page 401

---

**set service-profile use-client-dscp**

Configures MSS to classify the QoS level of IP packets based on their DSCP value, instead of their 802.11 priority.

**Syntax** — set service-profile name user-client-dscp {enable | disable}

- **name** — Service profile name.
- **enabled** — Enables mapping QoS level from the DSCP level.
- **disabled** — Disables mapping QoS level from the DSCP level.

**Defaults** — Disabled.

**Access** — Enabled.

**History** — Introduced in MSS Version 6.0.
set service-profile user-idle-timeout

**History** — If this command is enabled in the service profile, the 802.11 QoS level is ignored, and MSS classifies QoS level of IP packets based on their DSCP value.

**Examples** — The following command enables mapping the QoS level of IP packets based on their DSCP value for service profile sp1:

WX# set service-profile sp1 use-client-dscp enable
success: change accepted.

**See Also**
- `display service-profile` on page 401
- `display qos` on page 181

---

**set service-profile user-idle-timeout**

Changes the number of seconds MSS leaves a session up for a client that is not sending data and is not responding to keepalives (idle-client probes). If the timer expires, the client session is changed to the Dissociated state.

The timer is reset to 0 each time a client sends data or responds to an idle-client probe. If the idle-client probe is disabled, the timer is reset each time the client sends data.

**Syntax** — set service-profile name user-idle-timeout seconds

- **name** — Service profile name.
- **seconds** — Number of seconds a client is allowed to remain idle before MSS changes the session to the Dissociated state. You can specify from 20 to 86400 seconds.

To disable the timer, specify 0.

**Defaults** — The default user idle timeout is 180 seconds (3 minutes).

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Examples** — The following command increases the user idle timeout to 360 seconds (6 minutes):
set service-profile spl user-idle-timeout 360
success: change accepted.

See Also

- display service-profile on page 401
- set service-profile idle-client-probing on page 494
- set service-profile web-portal-session-timeout on page 525

**set service-profile web-portal-acl**  
Changes the ACL name MSS uses to filter Web-Portal user traffic during authentication.

Use this command if you create a custom Web-Portal ACL to allow more than just DHCP traffic during authentication. For example, if you configure an ACL that allows a Web-Portal user to access a credit card server, use this command to use the custom ACL for Web-Portal users that associate with the service profile SSID.

**Syntax — set service-profile name web-portal-acl aclname**

- **name**—Service profile name.
- **aclname**—Name of the ACL to use for filtering Web-Portal user traffic during authentication.

**Defaults —** By default, a service profile web-portal-acl option is not set. However, when you change the service profile auth-fallthru option to web-portal, MSS sets the web-portal-acl option to portalacl. (MSS automatically creates the portalacl ACL the first time you set any service profile auth-fallthru option to web-portal.)

**Access —** Enabled.

**History —** Introduced in MSS Version 5.0.

**Usage —** The first time you set the service profile auth-fallthru option to web-portal, MSS sets the web-portal-acl option to portalacl. The value remains portalacl even if you change the auth-fallthru option again. To change the web-portal-acl value, you must use the set service-profile web-portal-acl command.
The Web-Portal ACL applies only to users who log on using Web Portal, and applies only during authentication. After a Web Portal user is authenticated, the Web Portal ACL no longer applies. ACLs and other user attributes assigned to the username are applied instead.

**Examples** — The following command changes the Web-Portal ACL name to on service profile `sp3` to `creditsrvr`:

```
WX1200# set service-profile sp3 web-portal-acl creditsrvr
success: change accepted.
```

**See Also**

- `set service-profile auth-fallthru` on page 482
- `display service-profile` on page 401

### **set service-profile**

**web-portal-form**

Specifies a custom login page that loads for WebAAA users requesting the SSID managed by the service profile.

**Syntax** — `set service-profile name web-portal-form url`

- `name` — Service profile name.
- `url` — WX subdirectory name and HTML page name of the login page. Specify the full path. For example, `corpa-ssid/corpa.html`.

**Defaults** — The 3Com Web login page is served by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Option name changed from `web-aaa-form` to `web-portal-form`, to reflect change to portal-based implementation in MSS Version 4.0.

**Usage** — 3Com recommends that you create a subdirectory for the custom page and place all the page’s files in that subdirectory. Do not place the custom page in the root directory of the switch’s user file area.

If the custom login page includes gif or jpg images, their path names are interpreted relative to the directory from which the page is served.
To use WebAAA, the fallthru authentication type in the service profile that manages the SSID must be set to web. To use WebAAA for a wired authentication port, edit the port configuration with the set port type wired-auth command.

Examples — The following commands create a subdirectory named corpa-ssid, copy a custom login page named corpa-login.html and a jpg image named corpa-logo.jpg into that subdirectory, and set the Web login page for service profile to corpa-login.html:

WX4400# mkdir corpa-ssid
success: change accepted.
WX4400# copy tftp://10.1.1.1/corpa-login.html corpa-ssid/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
WX4400# copy tftp://10.1.1.1/corpa-logo.jpg corpa-ssid/corpa-logo.jpg
success: received 1202 bytes in 0.402 seconds [ 2112 bytes/sec]
WX4400# dir corpa-ssid
===============================================================================
file: Filename                        Size           Created
Total: 1839 bytes used, 206577 Kbytes free
WX4400# set service-profile corpa-service web-aaa-form corpa-ssid/corpa-login.html
success: change accepted.

See Also

- copy on page 715
- dir on page 718
- display service-profile on page 401
- mkdir on page 729
- set port type wired-auth on page 148
- set service-profile auth-fallthru on page 482
- set web-portal on page 326
set service-profile web-portal-logout logout-url

Specifies the URL that is requested when the user clicks the button to terminate his or her session in the Mobility Domain.

Syntax — set service-profile profile-name web-portal-logout logout-url url

- name — Service profile name.
- url — Specifies the URL for the Web Portal logout feature. The URL should be of the form https://host/logout.html.

Defaults — By default, the logout URL uses the IP address of the WX as the host part of the URL. The host can be either an IP address or a hostname.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — Specifying the URL for the Web Portal logout feature is useful if you want to standardize the URL across your network. For example, you can configure the logout URL on all of the WX switches in the Mobility Domain as wifizone.3Com.com/logout.html, where wifizone.3Com.com resolves to one of the WX switches in the Mobility Domain, ideally the seed.

To log out of the network, the user can click the “End Session” button in the pop-under window, or request the logout URL directly.

Standardizing the logout URL serves as a backup means for the user to log out in case the pop-under window is closed inadvertently. Note that if a user requests the logout URL, he or she must enter a username and password in order to identify the session on the WX. (This is not necessary when the user clicks the “End Session” button in the pop-under window.) Both the username and password are required to identify the session. If there is more than one session with the same username, then requesting the logout URL does not end any session.
Examples — The following command configures the Web Portal logout URL as: wifizone.3Com.com/logout.html for service profile sp1.

WX# set service-profile sp1 web-portal-logout logout-url https://wifizone.3Com.com/logout.html
success: change accepted.

See Also
- display service-profile on page 401
- set service-profile web-portal-logout mode on page 524

set service-profile web-portal-logout mode

Enables the Web Portal logout functionality, so that a user can manually terminate his or her session.

Syntax — set service-profile profile-name web-portal-logout mode {enable | disable}

- name — Service profile name.
- enabled — Enables the Web Portal logout functionality.
- disabled — Disables the Web Portal logout functionality.

Defaults — Disabled.

Access — Enabled.

History — Introduced in MSS Version 6.0.

Usage — When Web Portal logout functionality is enabled, after a Web Portal WebAAA user is successfully authenticated and redirected to the requested page, a pop-under window appears behind the user browser. The window contains a button labeled "End Session". When the user clicks this button, a URL is requested that terminates the user session in the Mobility Domain.

This feature allows Web Portal users a way to manually log out of the network, instead of waiting to be logged out automatically when the Web Portal WebAAA session timeout period expires.
set service-profile web-portal-session-timeout

**Examples** — The following command enables the Web Portal logout functionality for service profile `sp1`.

```
WX# set service-profile sp1 web-portal-logout mode enable
success: change accepted.
```

**See Also**
- `display service-profile` on page 401
- `set service-profile web-portal-logout logout-url` on page 523

---

`set service-profile web-portal-session-timeout`

Changes the number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically.

**Syntax** — `set service-profile name web-portal-session-timeout seconds`

- **name** — Service profile name.
- **seconds** — Number of seconds MSS allows Web Portal WebAAA sessions to remain in the Deassociated state before being terminated automatically. You can specify from 5 to 2800 seconds.

**Defaults** — The default Web Portal WebAAA session timeout is 5 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — When a client that has connected through Web Portal WebAAA enters standby or hibernation mode, the client may be idle for longer than the User idle-timeout period. When the User idle-timeout period expires, MSS places the client Web Portal WebAAA session in the Deassociated state. The Web Portal WebAAA session can remain in the Deassociated state for a configurable amount of time before being terminated automatically. This configurable amount of time is called the Web Portal WebAAA session timeout period. You can use this command to set the number of seconds in the Web Portal WebAAA session timeout period.
Note that the Web Portal WebAAA session timeout period applies only to Web Portal WebAAA sessions already authenticated with a username and password. For all other Web Portal WebAAA sessions, the default Web Portal WebAAA session timeout period of 5 seconds is used.

**Examples** — The following command allows Web Portal WebAAA sessions to remain in the Deassociated state 180 seconds before being terminated automatically.

```plaintext
WX4400# set service-profile sp1 web-portal-session-timeout 180
success: change accepted.
```

**See Also**

- `display service-profile` on page 401
- `set service-profile user-idle-timeout` on page 519

---

### set service-profile wep active-multicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting multicast frames.

**Syntax** — `set service-profile name wep active-multicast-index num`

- **name** — Service profile name.
- **num** — WEP key number. You can enter a value from 1 through 4.

**Defaults** — If WEP encryption is enabled and WEP keys are defined, MAP radios use WEP key 1 to encrypt multicast frames, by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Before using this command, you must configure values for the WEP keys you plan to use. Use the `set service-profile wep key-index` command.

**Examples** — The following command configures service profile sp2 to use WEP key 2 for encrypting multicast traffic:

```plaintext
WX4400# set service-profile sp2 wep active-multicast-index 2
success: change accepted.
```
set service-profile wep active-unicast-index

Specifies the static Wired-Equivalent Privacy (WEP) key (one of four) to use for encrypting unicast frames.

Syntax — set service-profile
name wep active-unicast-index num

- **name** — Service profile name.
- **num** — WEP key number. You can enter a value from 1 through 4.

Defaults — If WEP encryption is enabled and WEP keys are defined, MAP radios use WEP key 1 to encrypt unicast frames, by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Before using this command, you must configure values for the WEP keys you plan to use. Use the set service-profile wep key-index command.

Examples — The following command configures service profile sp2 to use WEP key 4 for encrypting unicast traffic:

WX4400# set service-profile sp2 wep active-unicast-index 4
success: change accepted.

See Also
- display service-profile on page 401
- set service-profile wep active-multicast-index on page 526
- set service-profile wep key-index on page 528
**set service-profile wep key-index**

Sets the value of one of four static Wired-Equivalent Privacy (WEP) keys for static WEP encryption.

**Syntax** — *set service-profile name wep key-index num key value*

- *name* — Service profile name.
- *key-index num* — WEP key index. You can enter a value from 1 through 4.
- *key value* — Hexadecimal value of the key. You can enter a 10-character ASCII string representing a 5-digit hexadecimal number or a 26-character ASCII string representing a 13-digit hexadecimal number. You can use numbers or letters. ASCII characters in the following ranges are supported:
  - 0 to 9
  - A to F
  - a to f

**Defaults** — By default, no static WEP keys are defined.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — MSS automatically enables static WEP when you define a WEP key. MSS continues to support dynamic WEP.

If you plan to use static WEP, do not map more than 8 service profiles that contain static WEP keys to the same radio profile.

**Examples** — The following command configures WEP key index 1 for service profile *sp2* to *aabbccddee*:

```
WX4400# set service-profile sp2 wep key-index 1 key aabbccddee
success: change accepted.
```

**See Also**

- *display service-profile* on page 401
- *set service-profile wep active-multicast-index* on page 526
- *set service-profile wep active-unicast-index* on page 527
**set service-profile wpa-ie**

Enables the WPA information element (IE) in wireless frames. The WPA IE advertises the WPA authentication methods and cipher suites supported by radios in the radio profile mapped to the service profile.

**Syntax** — `set service-profile name wpa-ie {enable | disable}`

- **name** — Service profile name.
- **enable** — Enables the WPA IE.
- **disable** — Disables the WPA IE.

**Defaults** — The WPA IE is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — When the WPA IE is enabled, the default authentication method is 802.1X. There is no default cipher suite. You must enable the cipher suites you want the radios to support.

**Examples** — The following command enables the WPA IE in service profile `sp2`:

```
WX4400# set service-profile sp2 wpa-ie enable
success: change accepted.
```

**See Also**

- [display service-profile](#) on page 401
- [set service-profile auth-dot1x](#) on page 481
- [set service-profile auth-psk](#) on page 483
- [set service-profile cipher-ccmp](#) on page 488
- [set service-profile cipher-tkip](#) on page 489
- [set service-profile cipher-wep104](#) on page 490
- [set service-profile cipher-wep40](#) on page 491
Use Spanning Tree Protocol (STP) commands to configure and manage spanning trees on the virtual LANs (VLANs) configured on a wireless LAN switch or controller, to maintain a loop-free network.

### STP Commands by Usage

This chapter presents STP commands alphabetically. Use the following table to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP State</td>
<td>set spantree on page 549</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display spantree on page 536</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display spantree blockedports on page 540</td>
<td></td>
</tr>
<tr>
<td>Bridge Priority</td>
<td>set spantree priority on page 558</td>
<td></td>
</tr>
<tr>
<td>Port Cost</td>
<td>set spantree portcost on page 553</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set spantree portvlancost on page 556</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display spantree portvlancost on page 542</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear spantree portcost on page 532</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear spantree portvlancost on page 533</td>
<td></td>
</tr>
<tr>
<td>Port Priority</td>
<td>set spantree portpri on page 555</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set spantree portvlanpri on page 557</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear spantree portpri on page 533</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear spantree portvlanpri on page 534</td>
<td></td>
</tr>
<tr>
<td>Timers</td>
<td>set spantree fwddelay on page 551</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set spantree hello on page 551</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set spantree maxage on page 552</td>
<td></td>
</tr>
<tr>
<td>Fast Convergence</td>
<td>set spantree portfast on page 554</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display spantree portfast on page 541</td>
<td></td>
</tr>
</tbody>
</table>
clear spantree portcost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge in all VLANs on a WX.

**Syntax** — `clear spantree portcost port-list`

- `port-list` — List of ports. The port cost is reset on the specified ports.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command resets the cost in all VLANs. To reset the cost for only specific VLANs, use the `clear spantree portvlancost` command.

**Examples** — The following command resets the STP port cost on ports 5 and 6 to the default value:

```
WX1200# clear spantree portcost 5-6
success: change accepted.
```

**See Also**
- `clear spantree portvlancost` on page 533
- `display spantree` on page 536
- `display spantree portvlancost` on page 542
- `set spantree portcost` on page 553
- `set spantree portvlancost` on page 556
clear spantree portpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge in all VLANs on a wireless LAN switch or controller.

**Syntax** — `clear spantree portpri port-list`

- `port-list` — List of ports. The port priority is reset to 32 (the default) on the specified ports.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command resets the priority in all VLANs. To reset the priority for only specific VLANs, use the `clear spantree portvlanpri` command.

**Examples** — The following command resets the STP priority on port 6 to the default:

```
WX1200# clear spantree portpri 6
success: change accepted.
```

**See Also**

- `clear spantree portvlanpri` on page 534
- `display spantree` on page 536
- `set spantree portpri` on page 555
- `set spantree portvlanpri` on page 557

---

clear spantree portvlancost

Resets to the default value the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a wireless LAN switch, or for all VLANs.

**Syntax** — `clear spantree portvlancost port-list {all | vlan vlan-id}`

- `port-list` — List of ports. The port cost is reset on the specified ports.
- `all` — Resets the cost for all VLANs.
- `vlan vlan-id` — VLAN name or number. MSS resets the cost for only the specified VLAN.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — MSS does not change a port's cost for VLANs other than the one(s) you specify.

**Examples** — The following command resets the STP cost for port 2 in VLAN sunflower:

```
WX4400# clear spantree portvlancost 2 vlan sunflower
success: change accepted.
```

**See Also**
- `clear spantree portcost` on page 532
- `display spantree` on page 536
- `display spantree portvlancost` on page 542
- `set spantree portcost` on page 553
- `set spantree portvlancost` on page 556

---

### clear spantree portvlanpri

Resets to the default value the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

**Syntax** — `clear spantree portvlanpri port-list { all | vlan vlan-id }`

- `port-list` — List of ports. The port priority is reset to 32 (the default) on the specified ports.
- `all` — Resets the priority for all VLANs.
- `vlan vlan-id` — VLAN name or number. MSS resets the priority for only the specified VLAN.

**Defaults** — None.

**Access** — Enabled.
clear spantree statistics

Clears STP statistics counters for a network port or ports and resets them to 0.

**Syntax** — `clear spantree statistics port-list [vlan vlan-id]`

- `port-list` — List of ports. Statistics counters are reset on the specified ports.
- `vlan vlan-id` — VLAN name or number. MSS resets statistics counters for only the specified VLAN.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command clears STP statistics counters for ports 1, 3, and 5 through 8, for all VLANs:

```
WX1200# clear spantree statistics 1,3,5-8
success: change accepted.
```

**See Also**
- `display spantree statistics` on page 542

---

**History** — Introduced in MSS Version 3.0.

**Usage** — MSS does not change a port’s priority for VLANs other than the one(s) you specify.

**Examples** — The following command resets the STP priority for port 2 in VLAN avocado:

```
WX4400# clear spantree portvlanpri 2 vlan avocado
success: change accepted.
```

**See Also**
- `clear spantree portpri` on page 533
- `display spantree` on page 536
- `set spantree portpri` on page 555
- `set spantree portvlanpri` on page 557
**display spantree**

Displays STP configuration and port-state information.

**Syntax** — `display spantree [port-list | vlan vlan-id] [active]`

- `port-list` — List of ports. If you do not specify any ports, MSS displays STP information for all ports.
- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays STP information for all VLANs.
- `active` — Displays information for only the active (forwarding) ports.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0. Version 4.2 added a value `STP Off` for STP-State and Port-State fields. This state indicates that STP is disabled on the port. The `Disabled` state is still used, but only to indicate that the port is not forwarding traffic.

**Examples** — The following command displays STP information for VLAN default:

```plaintext
WX1200# display spantree vlan default
VLAN   1
Spanning tree mode           PVST+
Spanning tree type           IEEE
Spanning tree enabled

Designated Root              00-02-4a-70-49-f7
Designated Root Priority     32768
Designated Root Path Cost  19
Designated Root Port         1
Root Max Age   20 sec   Hello Time 2 sec   Forward Delay 15 sec
Bridge ID MAC ADDR           00-0b-0e-02-76-f7
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan</th>
<th>STP-State</th>
<th>Cost</th>
<th>Prio</th>
<th>Portfast</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Forwarding</td>
<td>19</td>
<td>128</td>
<td>Disabled</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>STP Off</td>
<td>19</td>
<td>128</td>
<td>Disabled</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>Disabled</td>
<td>19</td>
<td>128</td>
<td>Disabled</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Disabled</td>
<td>19</td>
<td>128</td>
<td>Disabled</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Disabled</td>
<td>19</td>
<td>128</td>
<td>Disabled</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>Disabled</td>
<td>19</td>
<td>128</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Table 76 describes the fields in this display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>Spanning tree mode</td>
<td>In the current software version, the mode is always <strong>PVST+</strong>, which means Per VLAN Spanning Tree+.</td>
</tr>
<tr>
<td>Spanning tree type</td>
<td>In the current software version, the type is always <strong>IEEE 802</strong>, which means STP is based on the IEEE 802 standards.</td>
</tr>
<tr>
<td>Spanning tree enabled</td>
<td>State of STP on the VLAN.</td>
</tr>
<tr>
<td>Designated root</td>
<td>MAC address of the spanning tree’s root bridge.</td>
</tr>
<tr>
<td>Designated root priority</td>
<td>Bridge priority of the root bridge.</td>
</tr>
<tr>
<td>Designated root path cost</td>
<td>Cumulative cost from this bridge to the root bridge. If this WX switch is the root bridge, then the root cost is 0.</td>
</tr>
<tr>
<td>Designated root port</td>
<td>Port through which this WX switch reaches the root bridge. If this WX switch is the root bridge, this field says <em>We are the root</em>.</td>
</tr>
<tr>
<td>Root max age</td>
<td>Maximum acceptable age for hello packets on the root bridge.</td>
</tr>
<tr>
<td>Root hello time</td>
<td>Hello interval on the root bridge.</td>
</tr>
<tr>
<td>Root forward delay</td>
<td>Forwarding delay value on the root bridge.</td>
</tr>
<tr>
<td>Bridge Id mac addr</td>
<td>This WX switch’s MAC address.</td>
</tr>
<tr>
<td>Bridge Id priority</td>
<td>This WX switch’s bridge priority.</td>
</tr>
<tr>
<td>Bridge max age</td>
<td>This WX switch’s maximum acceptable age for hello packets.</td>
</tr>
<tr>
<td>Bridge hello time</td>
<td>This WX switch’s hello interval.</td>
</tr>
<tr>
<td>Bridge forward delay</td>
<td>This WX switch’s forwarding delay value.</td>
</tr>
</tbody>
</table>
Port number. Only network ports are listed. STP does not apply to 3Com Wireless LAN Managed Access Point AP2750 ports or wired authentication ports.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number. Only network ports are listed. STP does not apply to 3Com Wireless LAN Managed Access Point AP2750 ports or wired authentication ports.</td>
</tr>
<tr>
<td>Vlan</td>
<td>VLAN ID.</td>
</tr>
<tr>
<td>STP-State</td>
<td>STP state of the port:</td>
</tr>
<tr>
<td>or Port-State</td>
<td>Blocking—The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic.</td>
</tr>
<tr>
<td></td>
<td>Disabled—This state can indicate any of the following conditions:</td>
</tr>
<tr>
<td></td>
<td>■ The port is inactive.</td>
</tr>
<tr>
<td></td>
<td>■ The port is disabled.</td>
</tr>
<tr>
<td></td>
<td>■ STP is enabled on the port but the port is not forwarding traffic. (The port is active and enabled but STP has just started to come up.)</td>
</tr>
<tr>
<td></td>
<td>■ Forwarding—The port is forwarding Layer 2 traffic.</td>
</tr>
<tr>
<td></td>
<td>■ Learning—The port is learning the locations of other devices in the spanning tree before changing state to forwarding.</td>
</tr>
<tr>
<td></td>
<td>■ Listening—The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.</td>
</tr>
<tr>
<td></td>
<td>■ STP Off—STP is disabled on the port.</td>
</tr>
</tbody>
</table>
**display spantree backbonefast**

Indicates whether the STP backbone fast convergence feature is enabled or disabled.

**Syntax** — `display spantree backbonefast`

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

---

**Table 76  Output for display spantree (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-state</td>
<td>STP state of the port:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Blocking</strong> — The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Disabled</strong> — The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Forwarding</strong> — The port is forwarding Layer 2 traffic.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Learning</strong> — The port is learning the locations of other WX switches in the spanning tree before changing state to forwarding.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Listening</strong> — The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>STP Off</strong> — STP is disabled on the port.</td>
</tr>
<tr>
<td>Cost</td>
<td>STP cost of the port.</td>
</tr>
<tr>
<td>Prio</td>
<td>STP priority of the port.</td>
</tr>
<tr>
<td>Portfast</td>
<td>State of the uplink fast convergence feature:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Enabled</strong></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Disabled</strong></td>
</tr>
</tbody>
</table>

**See Also**

- **display spantree blockedports** on page 540
Examples — The following example shows the command output on a WX switch with backbone fast convergence enabled:

WX4400# display spantree backbonefast

Backbonefast is enabled

See Also
- set spantree backbonefast on page 550

display spantree blockedports

Lists information about wireless LAN switch ports that STP has blocked on one or all of its VLANs.

Syntax — display spantree blockedports [vlan vlan-id]

- vlan vlan-id — VLAN name or number. If you do not specify a VLAN, MSS displays information for blocked ports on all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Usage — The command lists information separately for each VLAN.

Examples — The following command shows information about blocked ports on a WX switch for the default VLAN (VLAN 1):

WX4400# display spantree blockedports vlan default

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan</th>
<th>Port-State</th>
<th>Cost</th>
<th>Prio</th>
<th>Portfast</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>190</td>
<td>Blocking</td>
<td>4</td>
<td>128</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Number of blocked ports (segments) in VLAN 1 : 1

The port information is the same as the information displayed by the display spantree command. See Table 76 on page 537.

See Also
- display spantree on page 536
display spantree portfast

Displays STP uplink fast convergence information for all network ports or for one or more network ports.

Syntax — display spantree portfast [port-list]

- port-list — List of ports. If you do not specify any ports, MSS displays uplink fast convergence information for all ports.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command shows uplink fast convergence information for all ports:

```
WX1200# display spantree portfast
Port          VLAN  Portfast
------------------------- ----   ----------
1              1      disable
2              1      disable
3              1      disable
4              1      enable
5              1      disable
6              1      disable
7              1      disable
8              1      disable
```

Table 77 describes the fields in this display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>Portfast</td>
<td>State of the uplink fast convergence feature:</td>
</tr>
<tr>
<td></td>
<td>■ Enable</td>
</tr>
<tr>
<td></td>
<td>■ Disable</td>
</tr>
</tbody>
</table>

See Also

- set spantree portfast on page 554
**display spantree portvlancost**

Shows the cost of a port on a path to the STP root bridge, for each of the port's VLANs.

**Syntax** — `display spantree portvlancost port-list`

- `port-list` — List of ports.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command shows the STP port cost of port 1:

```
WX4400# display spantree portvlancost 1
port 1 VLAN 1 have path cost 19
```

**See Also**

- `clear spantree portcost` on page 532
- `clear spantree portvlancost` on page 533
- `display spantree` on page 536
- `set spantree portcost` on page 553
- `set spantree portvlancost` on page 556

**display spantree statistics**

Displays STP statistics for one or more WX network ports.

**Syntax** — `display spantree statistics [port-list [vlan vlan-id]]`

- `port-list` — List of ports. If you do not specify any ports, MSS displays STP statistics for all ports.
- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.
**Usage** — The command displays statistics separately for each port.

**Examples** — The following command shows STP statistics for port 1:

```bash
WX4400# display spantree statistics 1
```

**BPDU related parameters**

Port 1      VLAN 1  
spanning tree enabled for VLAN = 1
port spanning tree enabled  
state          Forwarding
port_id        0x8015
port_number     0x5
path cost       0x4
message age (port/VLAN) 0(20)
designated_root 00-0b-0e-00-04-30
designated cost 0x0
designated bridge 00-0b-0e-00-04-30
designated port  38
top_change_ack   FALSE
config_pending   FALSE
port_inconsistency none

**Port based information statistics**

- config BPDU’s xmitted(port/VLAN) 0 (1)
- config BPDU’s received(port/VLAN) 21825 (43649)
- tcn BPDU’s xmitted(port/VLAN) 0 (0)
- tcn BPDU’s received(port/VLAN) 2 (2)
- forward transition count (port/VLAN) 1 (1)
- scp failure count 0
- root inc trans count (port/VLAN) 1 (1)
- inhibit loopguard FALSE
- loop inc trans count 0 (0)

**Status of Port Timers**

- forward delay timer INACTIVE
- forward delay timer value 15
- message age timer ACTIVE
- message age timer value 0
- topology change timer INACTIVE
topology change timer value              0
hold timer                               INACTIVE
hold timer value                         0
delay root port timer                    INACTIVE
delay root port timer value              0
delay root port timer restarted is       FALSE

VLAN based information & statistics

spanning tree type                        ieee
spanning tree multicast address          01-00-0c-cc-cc-cd
bridge priority                          32768
bridge MAC address                       00-0b-0e-12-34-56
bridge hello time                        2
bridge forward delay                     15
topology change initiator:               0
last topology change occured:            Tue Jul 01 2003 22:33:36.
topology change                          FALSE
topology change time                     35
topology change detected                 FALSE
topology change count                    1
topology change last recvd. from         00-0b-0e-02-76-f6

Other port specific info

dynamic max age transition               0
port BPDU ok count                       21825
msg age expiry count                     0
link loading                             0
BPDU in processing                       FALSE
num of similar BPDU's to process         0
received_inferior_bpdu                   FALSE
next state                               0
src MAC count                            21807
total src MAC count                      21825
curr_src_mac                             00-0b-0e-00-04-30
next_src_mac                             00-0b-0e-02-76-f6

Table 78 describes the fields in this display.
Table 78  Output for display spantree statistics

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number.</td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN ID.</td>
</tr>
<tr>
<td>Spanning Tree enabled for vlan</td>
<td>State of the STP feature on the VLAN.</td>
</tr>
<tr>
<td>port spanning tree</td>
<td>State of the STP feature on the port.</td>
</tr>
<tr>
<td>state</td>
<td>STP state of the port:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Blocking</strong> — The port is not forwarding Layer 2 traffic but is listening to and forwarding STP control traffic.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disabled</strong> — The port is not forwarding any traffic, including STP control traffic. The port might be administratively disabled or the link might be disconnected.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Forwarding</strong> — The port is forwarding Layer 2 traffic.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Learning</strong> — The port is learning the locations of other WX switches in the spanning tree before changing state to forwarding.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Listening</strong> — The port is comparing its own STP information with information in STP control packets received by the port to compute the spanning tree and change state to blocking or forwarding.</td>
</tr>
<tr>
<td>port_id</td>
<td>STP port ID.</td>
</tr>
<tr>
<td>port_number</td>
<td>STP port number.</td>
</tr>
<tr>
<td>path cost</td>
<td>Cost to use this port to reach the root bridge. This is part of the total path cost (designated cost).</td>
</tr>
<tr>
<td>message age</td>
<td>Age of the protocol information for a port and the value of the maximum age parameter (shown in parenthesis) recorded by the switch.</td>
</tr>
<tr>
<td>designated_root</td>
<td>MAC address of the root bridge.</td>
</tr>
<tr>
<td>designated cost</td>
<td>Total path cost to reach the root bridge.</td>
</tr>
<tr>
<td>designated_bridge</td>
<td>Bridge to which this switch forwards traffic away from the root bridge.</td>
</tr>
<tr>
<td>designated_port</td>
<td>STP port through which this switch forwards traffic away from the root bridge.</td>
</tr>
<tr>
<td>top_change_ack</td>
<td>Value of the topology change acknowledgment flag in the next configured bridge protocol data unit (BPDU) to be transmitted on the associated port. The flag is set in reply to a topology change notification BPDU.</td>
</tr>
</tbody>
</table>
### Table 78  Output for display spantree statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config_pending</td>
<td>Indicates whether a configured BPDU is to be transmitted on expiration of the hold timer for the port.</td>
</tr>
<tr>
<td>port_inconsistency</td>
<td>Indicates whether the port is in an inconsistent state.</td>
</tr>
<tr>
<td>config BPDU’s xmitted</td>
<td>Number of BPDUs transmitted from the port. A number in parentheses indicates the number of configured BPDUs transmitted by the WX switch for this VLAN’s spanning tree.</td>
</tr>
<tr>
<td>config BPDU’s received</td>
<td>Number of BPDUs received by this port. A number in parentheses indicates the number of configured BPDUs received by the WX switch for this VLAN’s spanning tree.</td>
</tr>
<tr>
<td>tcn BPDU’s xmitted</td>
<td>Number of topology change notification (TCN) BPDUs transmitted on this port.</td>
</tr>
<tr>
<td>tcn BPDU’s received</td>
<td>Number of TCN BPDUs received on this port.</td>
</tr>
<tr>
<td>forward transition count</td>
<td>Number of times the port state transitioned to the forwarding state.</td>
</tr>
<tr>
<td>scp failure count</td>
<td>Number of service control point (SCP) failures.</td>
</tr>
<tr>
<td>root inc trans count</td>
<td>Number of times the root bridge changed.</td>
</tr>
<tr>
<td>inhibit loopguard</td>
<td>State of the loop guard. In the current release, the state is always FALSE.</td>
</tr>
<tr>
<td>loop inc trans count</td>
<td>Number of loops that have occurred.</td>
</tr>
<tr>
<td>forward delay timer</td>
<td>Status of the forwarding delay timer. This timer monitors the time spent by a port in the listening and learning states.</td>
</tr>
<tr>
<td>forward delay timer value</td>
<td>Current value of the forwarding delay timer, in seconds.</td>
</tr>
<tr>
<td>message age timer</td>
<td>Status of the message age timer. This timer measures the age of the received protocol information recorded for a port.</td>
</tr>
<tr>
<td>message age timer value</td>
<td>Current value of the message age timer, in seconds.</td>
</tr>
<tr>
<td>topology change timer</td>
<td>Status of the topology change timer. This timer determines the time period during which configured BPDUs are transmitted with the topology change flag set by this WX switch when it is the root bridge, after detection of a topology change.</td>
</tr>
<tr>
<td>topology change timer value</td>
<td>Current value of the topology change timer, in seconds.</td>
</tr>
</tbody>
</table>
Table 78  Output for display spantree statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hold timer</td>
<td>Status of the hold timer. This timer ensures that configured BPDUs are not transmitted too frequently through any bridge port.</td>
</tr>
<tr>
<td>hold timer value</td>
<td>Current value of the hold timer, in seconds.</td>
</tr>
<tr>
<td>delay root port timer</td>
<td>Status of the delay root port timer, which enables fast convergence when uplink fast convergence is enabled.</td>
</tr>
<tr>
<td>delay root port timer value</td>
<td>Current value of the delay root port timer.</td>
</tr>
<tr>
<td>delay root port timer restarted is</td>
<td>Whether the delay root port timer has been restarted.</td>
</tr>
<tr>
<td>spanning tree type</td>
<td>Type of spanning tree. The type is always IEEE.</td>
</tr>
<tr>
<td>spanning tree multicast address</td>
<td>Destination address used to send out configured BPDUs on a bridge port.</td>
</tr>
<tr>
<td>bridge priority</td>
<td>STP priority of this WX switch.</td>
</tr>
<tr>
<td>bridge MAC address</td>
<td>MAC address of this WX switch.</td>
</tr>
<tr>
<td>bridge hello time</td>
<td>Value of the hello timer interval, in seconds, when this WX switch is the root or is attempting to become the root.</td>
</tr>
<tr>
<td>bridge forward delay</td>
<td>Value of the forwarding delay interval, in seconds, when this WX switch is the root or is attempting to become the root.</td>
</tr>
<tr>
<td>topology change initiator</td>
<td>Port number that initiated the most recent topology change.</td>
</tr>
<tr>
<td>last topology change occurred</td>
<td>System time when the most recent topology change occurred.</td>
</tr>
<tr>
<td>topology change</td>
<td>Value of the topology change flag in configuration BPDUs to be transmitted by this WX switch on VLANs for which the switch is the designated bridge.</td>
</tr>
<tr>
<td>topology change time</td>
<td>Time period, in seconds, during which BPDUs are transmitted with the topology change flag set by this WX switch when it is the root bridge, after detection of a topology change. It is equal to the sum of the switch’s maximum age and forwarding delay parameters.</td>
</tr>
<tr>
<td>topology change detected</td>
<td>Indicates whether a topology change has been detected by the switch.</td>
</tr>
<tr>
<td>topology change count</td>
<td>Number of times the topology change has occurred.</td>
</tr>
<tr>
<td>topology change last recv. from</td>
<td>MAC address of the bridge from which the WX switch last received a topology change.</td>
</tr>
<tr>
<td>dynamic max age transition</td>
<td>Number of times the maximum age parameter was changed dynamically.</td>
</tr>
</tbody>
</table>
display spantree uplinkfast

Shows uplink fast convergence information for one VLAN or all VLANs.

Syntax — display spantree uplinkfast [vlan vlan-id]

- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, MSS displays STP statistics for all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command shows uplink fast convergence information for all VLANs:

```
WX4400# display spantree uplinkfast
VLAN    port    list
--------------------------------------------------------------
1       1(fwd),2,3
```

Table 79 describes the fields in this display.
set spantree

Enables or disables STP on one VLAN or all VLANs configured on a WX switch.

**Syntax** — set spantree {enable | disable } [{all | vlan vlan-id | port port-list vlan-id}]

- **enable** — Enables STP.
- **disable** — Disables STP.
- **all** — Enables or disables STP on all VLANs.
- **vlan vlan-id** — VLAN name or number. MSS enables or disables STP on only the specified VLAN, on all ports within the VLAN.
- **port port-list vlan-id** — Port number or list and the VLAN the ports are in. MSS enables or disables STP on only the specified ports, within the specified VLAN.

**Defaults** — Disabled.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command enables STP on all VLANs configured on a WX switch:

```
WX4400# set spantree enable
success: change accepted.
```

The following command disables STP on VLAN burgundy:

```
WX4400# set spantree disable vlan burgundy
success: change accepted.
```
See Also

- display spantree on page 536

**set spantree backbonefast**

Enables or disables STP backbone fast convergence on a wireless LAN switch. This feature accelerates a port’s recovery following the failure of an indirect link.

⚠️ **CAUTION:** The backbone fast convergence feature is not compatible with switches that are running standard IEEE 802.1D Spanning Tree implementations. This includes switches running Rapid Spanning Tree or Multiple Spanning Tree.

**Syntax** — set spantree backbonefast {enable | disable}

- **enable** — Enables backbone fast convergence.
- **disable** — Disables backbone fast convergence.

**Defaults** — STP backbone fast path convergence is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — If you plan to use the backbone fast convergence feature, you must enable it on all the bridges in the spanning tree.

**Examples** — The following command enables backbone fast convergence:

WX4400# set spantree backbonefast enable
success: change accepted.

See Also

- display spantree backbonefast on page 539
Changes the period of time after a topology change that a WX switch which is not the root bridge waits to begin forwarding Layer 2 traffic on one or all of its configured VLANs. (The root bridge always forwards traffic.)

Syntax — set spantree fwddelay delay {all | vlan vlan-id}
- delay — Delay value. You can specify from 4 through 30 seconds.
- all — Changes the forwarding delay on all VLANs.
- vlan vlan-id — VLAN name or number. MSS changes the forwarding delay on only the specified VLAN.

Defaults — The default forwarding delay is 15 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the forwarding delay on VLAN pink to 20 seconds:
WX4400# set spantree fwddelay 20 vlan pink
success: change accepted.

See Also
- display spantree on page 536

Changes the interval between STP hello messages sent by a wireless LAN switch when operating as the root bridge, on one or all of its configured VLANs.

Syntax — set spantree hello interval {all | vlan vlan-id}
- interval — Interval value. You can specify from 1 through 10 seconds.
- all — Changes the interval on all VLANs.
- vlan vlan-id — VLAN name or number. MSS changes the interval on only the specified VLAN.

Defaults — The default hello timer interval is 2 seconds.
Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the hello interval for all VLANs to 4 seconds:

```
WX4400# set spantree hello 4 all
success: change accepted.
```

See Also

- `display spantree` on page 536

---

**set spantree maxage**

Changes the maximum age for an STP root bridge hello packet that is acceptable to a wireless LAN switch acting as a designated bridge on one or all of its VLANs. After waiting this period of time for a new hello packet, the WX switch determines that the root bridge is unavailable and issues a topology change message.

Syntax — `set spantree maxage aging-time {all | vlan vlan-id}

- `aging-time` — Maximum age value. You can specify from 6 through 40 seconds.
- `all` — Changes the maximum age on all VLANs.
- `vlan vlan-id` — VLAN name or number. MSS changes the maximum age on only the specified VLAN.

Defaults — The default maximum age for root bridge hello packets is 20 seconds.

Access — Enabled.

History —Introduced in MSS Version 3.0.

Examples — The following command changes the maximum acceptable age for root bridge hello packets on all VLANs to 15 seconds:

```
WX4400# set spantree maxage 15 all
success: change accepted.
```

See Also

- `display spantree` on page 536
set spantree portcost

Changes the cost that transmission through a network port or ports in
the default VLAN on a wireless LAN switch adds to the total cost of a
path to the STP root bridge.

Syntax — set spantree portcost port-list cost cost
  port-list — List of ports. MSS applies the cost change to all the
  specified ports.
  cost cost — Numeric value. You can specify a value from 1 through
  65,535. STP selects lower-cost paths over higher-cost paths.

Defaults — The default port cost depends on the port speed and link
type. Table 80 lists the defaults for STP port path cost.

Table 80  SNMP Port Path Cost Defaults

<table>
<thead>
<tr>
<th>Port Speed</th>
<th>Link Type</th>
<th>Default Port Path Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000 Mbps</td>
<td>Full Duplex Aggregate Link (Port Group)</td>
<td>19</td>
</tr>
<tr>
<td>1000 Mbps</td>
<td>Full Duplex</td>
<td>4</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>Full Duplex Aggregate Link (Port Group)</td>
<td>19</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>Full Duplex</td>
<td>18</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>Half Duplex</td>
<td>19</td>
</tr>
<tr>
<td>10 Mbps</td>
<td>Full Duplex Aggregate Link (Port Group)</td>
<td>19</td>
</tr>
<tr>
<td>10 Mbps</td>
<td>Full Duplex</td>
<td>95</td>
</tr>
<tr>
<td>10 Mbps</td>
<td>Half Duplex</td>
<td>100</td>
</tr>
</tbody>
</table>

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command applies only to the default VLAN (VLAN 1). To
tchange the cost of a port in another VLAN, use the set spantree
portvlancost command.

Examples — The following command changes the cost on ports 3 and 4
to 20:

WX1200# set spantree portcost 3,4 cost 20
success: change accepted.
See Also

- clear spantree portcost on page 532
- clear spantree portvlancost on page 533
- display spantree on page 536
- display spantree portvlancost on page 542
- set spantree portvlancost on page 556

---

**set spantree portfast**

Enables or disables STP port fast convergence on one or more ports on a wireless LAN switch.

**Syntax** — set spantree portfast port port-list {enable | disable}

- **port** port-list — List of ports. MSS enables the feature on the specified ports.
- **enable** — Enables port fast convergence.
- **disable** — Disables port fast convergence.

**Defaults** — STP port fast convergence is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Use port fast convergence on ports that are directly connected to servers, hosts, or other MAC stations.

**Examples** — The following command enables port fast convergence on ports 2, 5, and 7:

```
WX1200# set spantree portfast port 2,4,7 enable
success: change accepted.
```

See Also

- display spantree portfast on page 541
set spantree portpri

Changes the STP priority of a network port or ports for selection as part of the path to the STP root bridge in the default VLAN on a wireless LAN switch.

Syntax — set spantree portpri port-list priority value
- **port-list** — List of ports. MSS changes the priority on the specified ports.
- **priority value** — Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).

Defaults — The default STP priority for all network ports is 128.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command applies only to the default VLAN (VLAN 1). To change the priority of a port in another VLAN, use the set spantree portvlanpri command.

Examples — The following command sets the priority of ports 3 and 4 to 48:

WX1200# set spantree portpri 3-4 priority 48
success: change accepted.

See Also
- clear spantree portpri on page 533
- clear spantree portvlanpri on page 534
- display spantree on page 536
- set spantree portvlanpri on page 557
set spantree portvlancost

Changes the cost of a network port or ports on paths to the STP root bridge for a specific VLAN on a wireless LAN switch.

Syntax — set spantree portvlancost port-list cost cost {all | vlan vlan-id}

- port-list — List of ports. MSS applies the cost change to all the specified ports.
- cost cost — Numeric value. You can specify a value from 1 through 65,535. STP selects lower-cost paths over higher-cost paths.
- all — Changes the cost on all VLANs.
- vlan vlan-id — VLAN name or number. MSS changes the cost on only the specified VLAN.

Defaults — The default port cost depends on the port speed and link type. (See Table 75 on page 531.)

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command changes the cost on ports 3 and 4 to 20 in VLAN mauve:

WX1200# set spantree portvlancost 3,4 cost 20 vlan mauve
success: change accepted.

See Also

- clear spantree portcost on page 532
- clear spantree portvlancost on page 533
- display spantree on page 536
- display spantree portvlancost on page 542
- set spantree portcost on page 553
set spantree portvlanpri

Changes the priority of a network port or ports for selection as part of the path to the STP root bridge, on one VLAN or all VLANs.

**Syntax** — `set spantree portvlanpri port-list priority value {all | vlan vlan-id}`

- `port-list` — List of ports. MSS changes the priority on the specified ports.
- `priority value` — Priority value. You can specify a value from 0 (highest priority) through 255 (lowest priority).
- `all` — Changes the priority on all VLANs.
- `vlan vlan-id` — VLAN name or number. MSS changes the priority on only the specified VLAN.

**Defaults** — The default STP priority for all network ports is 128.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command sets the priority of ports 3 and 4 to 48 on VLAN mauve:

```
WX1200# set spantree portvlanpri 3-4 priority 48 vlan mauve
success: change accepted.
```

**See Also**

- `clear spantree portpri` on page 533
- `clear spantree portvlanpri` on page 534
- `display spantree` on page 536
- `set spantree portpri` on page 555
**set spantree priority**

Changes the STP root bridge priority of a wireless LAN switch on one or all of its VLANs.

**Syntax** — `set spantree priority value {all | vlan vlan-id}`

- `priority value` — Priority value. You can specify a value from 0 through 65,535. The bridge with the lowest priority value is elected to be the root bridge for the spanning tree.
- `all` — Changes the bridge priority on all VLANs.
- `vlan vlan-id` — VLAN name or number. MSS changes the bridge priority on only the specified VLAN.

**Defaults** — The default root bridge priority for the switch on all VLANs is 32,768.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command sets the bridge priority of VLAN pink to 69:

```
WX4400# set spantree priority 69 vlan pink
success: change accepted.
```

**See Also**

- display spantree on page 536

**set spantree uplinkfast**

Enables or disables STP uplink fast convergence on a wireless LAN switch. This feature enables a WX switch with redundant links to the network backbone to immediately switch to the backup link to the root bridge if the primary link fails.

**Syntax** — `set spantree uplinkfast {enable | disable}`

- `enable` — Enables uplink fast convergence.
- `disable` — Disables uplink fast convergence.

**Defaults** — Disabled.

**Access** — Enabled.
History — Introduced in MSS Version 3.0.

Usage — The uplink fast convergence feature is applicable to bridges that are acting as access switches to the network core (distribution layer) but are not in the core themselves. Do not enable the feature on WX switches that are in the network core.

Examples — The following command enables uplink fast convergence:

```
WX4400# set spantree uplinkfast enable
success: change accepted.
```

See Also
- `display spantree uplinkfast` on page 548
13 IGMP Snooping Commands

Use Internet Group Management Protocol (IGMP) snooping commands to configure and manage multicast traffic reduction on a WX.

This chapter presents IGMP snooping commands alphabetically. Use the following table to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Snooping State</td>
<td>set igmp on page 573</td>
</tr>
<tr>
<td></td>
<td>display igmp on page 562</td>
</tr>
<tr>
<td>Proxy Reporting</td>
<td>set igmp proxy-report on page 578</td>
</tr>
<tr>
<td>Pseudo-querier</td>
<td>set igmp querier on page 581</td>
</tr>
<tr>
<td></td>
<td>display igmp querier on page 567</td>
</tr>
<tr>
<td>Timers</td>
<td>set igmp qi on page 579</td>
</tr>
<tr>
<td></td>
<td>set igmp oqi on page 577</td>
</tr>
<tr>
<td></td>
<td>set igmp qri on page 580</td>
</tr>
<tr>
<td></td>
<td>set igmp lmqi on page 574</td>
</tr>
<tr>
<td></td>
<td>set igmp rv on page 582</td>
</tr>
<tr>
<td>Router Solicitation</td>
<td>set igmp mrsol on page 576</td>
</tr>
<tr>
<td></td>
<td>set igmp mrsol mrsi on page 576</td>
</tr>
<tr>
<td>Multicast Routers</td>
<td>set igmp mrouter on page 575</td>
</tr>
<tr>
<td></td>
<td>display igmp mrouter on page 566</td>
</tr>
<tr>
<td>Multicast Receivers</td>
<td>set igmp receiver on page 581</td>
</tr>
<tr>
<td></td>
<td>display igmp receiver-table on page 569</td>
</tr>
<tr>
<td>Statistics</td>
<td>display igmp statistics on page 571</td>
</tr>
<tr>
<td></td>
<td>clear igmp statistics on page 562</td>
</tr>
</tbody>
</table>
clear igmp statistics  Clears IGMP statistics counters on one VLAN or all VLANs on a wireless LAN switch and resets them to 0.

Syntax — clear igmp statistics [vlan vlan-id]

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, IGMP statistics are cleared for all VLANs.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command clears IGMP statistics for all VLANs:

```
WX1200# clear igmp statistics
IGMP statistics cleared for all vlans
```

See Also — display igmp statistics on page 571

display igmp  Displays IGMP configuration information and statistics.

Syntax — display igmp [vlan vlan-id]

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays IGMP information for all VLANs.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.
Examples — The following command displays IGMP information for VLAN orange:

WX1200# display igmp vlan orange
VLAN: orange
IGMP is enabled
Proxy reporting is on
Mrouter solicitation is on
Querier functionality is off
Configuration values: qi: 125 oqi: 300 qri: 100 lmqi: 10 rvalue: 2 Multicast router information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Mrouter-IPaddr</th>
<th>Mrouter-MAC</th>
<th>Type</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.28.7.5</td>
<td>00:01:02:03:04:05</td>
<td>dvmrp</td>
<td>17</td>
</tr>
</tbody>
</table>

Group | Port | Receiver-IP | Receiver-MAC | TTL |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.2</td>
<td>none</td>
<td>none</td>
<td>none</td>
<td>undef</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Querier-IP</th>
<th>Querier-MAC</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>193.122.135.178</td>
<td>00:0b:cc:d2:e9:b4</td>
<td>23</td>
</tr>
</tbody>
</table>

IGMP vlan member ports: 1, 2, 3
IGMP static ports: none
IGMP static information:

IGMP message type Received Transmitted Dropped
----------------- -------- ----------- -------
General-Queries 0 0 0
GS-Queries 0 0 0
Report V1 0 0 0
Report V2 5 1 4
Leave 0 0 0
Mrouter-Adv 0 0 0
Mrouter-Term 0 0 0
Mrouter-Sol 50 101 0
DVMRP 4 4 0
PIM V1 0 0 0
PIM V2 0 0 0
Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
Table 82 describes the fields in this display.

### Table 82  Output for display igmp

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN name. MSS displays information separately for each VLAN.</td>
</tr>
<tr>
<td>IGMP is enabled (disabled)</td>
<td>IGMP state.</td>
</tr>
<tr>
<td>Proxy reporting</td>
<td>Proxy reporting state.</td>
</tr>
<tr>
<td>Mrouter solicitation</td>
<td>Multicast router solicitation state.</td>
</tr>
<tr>
<td>Querier functionality</td>
<td>Pseudo-querier state.</td>
</tr>
<tr>
<td>Configuration values (qi)</td>
<td>Query interval.</td>
</tr>
<tr>
<td>Configuration values (oqi)</td>
<td>Other-querier-present interval.</td>
</tr>
<tr>
<td>Configuration values (qri)</td>
<td>Query response interval.</td>
</tr>
<tr>
<td>Configuration values (lmqi)</td>
<td>Last member query interval.</td>
</tr>
<tr>
<td>Configuration values (rvalue)</td>
<td>Robustness value.</td>
</tr>
<tr>
<td>Multicast router information</td>
<td>List of multicast routers and active multicast groups. The fields containing this information are described separately. The <strong>display igmp mrouter</strong> command shows the same information.</td>
</tr>
<tr>
<td>Port</td>
<td>Number of the physical port through which the WX can reach the router.</td>
</tr>
<tr>
<td>Mrouter-IPaddr</td>
<td>IP address of the multicast router interface.</td>
</tr>
<tr>
<td>Mrouter-MAC</td>
<td>MAC address of the multicast router interface.</td>
</tr>
<tr>
<td>Type</td>
<td>How the WX learned that the port is a multicast router port:</td>
</tr>
<tr>
<td></td>
<td>• <strong>conf</strong> — Static multicast port configured by an administrator</td>
</tr>
<tr>
<td></td>
<td>• <strong>madv</strong> — Multicast advertisement</td>
</tr>
<tr>
<td></td>
<td>• <strong>quer</strong> — IGMP query</td>
</tr>
<tr>
<td></td>
<td>• <strong>dvmrp</strong> — Distance Vector Multicast Routing Protocol (DVMRP)</td>
</tr>
<tr>
<td></td>
<td>• <strong>pimv1</strong> — Protocol Independent Multicast (PIM) version 1</td>
</tr>
<tr>
<td></td>
<td>• <strong>pimv2</strong> — PIM version 2</td>
</tr>
</tbody>
</table>
Table 82  Output for display igmp (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL</td>
<td>Number of seconds before this entry ages out if not refreshed. For static multicast router entries, the time-to-live (TTL) value is <em>undef</em>. Static multicast router entries do not age out.</td>
</tr>
<tr>
<td>Group</td>
<td>IP address of a multicast group. The <code>display igmp receiver-table</code> command shows the same information as these receiver fields.</td>
</tr>
<tr>
<td>Port</td>
<td>Physical port through which the WX can reach the group’s receiver.</td>
</tr>
<tr>
<td>Receiver-IP</td>
<td>IP address of the client receiving the group.</td>
</tr>
<tr>
<td>Receiver-MAC</td>
<td>MAC address of the client receiving the group.</td>
</tr>
<tr>
<td>TTL</td>
<td>Number of seconds before this entry ages out if the WX does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is <em>undef</em>. Static multicast receiver entries do not age out.</td>
</tr>
<tr>
<td>Querier information</td>
<td>Information about the subnet’s multicast querier. If the querier is another WX switch, the fields described below are applicable. If the querier is the WX itself, the output indicates how many seconds remain until the next general query message. If IGMP snooping does not detect a querier, the output indicates this. The <code>display igmp querier</code> command shows the same information.</td>
</tr>
<tr>
<td>Querier for vlan</td>
<td>VLAN containing the querier. Information is listed separately for each VLAN.</td>
</tr>
<tr>
<td>Querier-IP</td>
<td>IP address of the querier.</td>
</tr>
<tr>
<td>Querier-MAC</td>
<td>MAC address of the querier.</td>
</tr>
<tr>
<td>TTL</td>
<td>Number of seconds before this entry ages out if the WX does not receive a query message from the querier.</td>
</tr>
<tr>
<td>IGMP vlan member ports</td>
<td>Physical ports in the VLAN. This list includes all network ports configured to be in the VLAN and all ports MSS dynamically assigns to the VLAN when a user assigned to the VLAN becomes a receiver. For example, the list can include a MAP access port that is not configured to be in the VLAN when a user associated with the 3Com Wireless LAN Managed Access Point AP2750 on that port becomes a receiver for a group. When all receivers on a dynamically added port age out, MSS removes the port from the list.</td>
</tr>
<tr>
<td>IGMP static ports</td>
<td>Static receiver ports.</td>
</tr>
<tr>
<td>IGMP statistics</td>
<td>Multicast message and packet statistics. These are the same statistics displayed by the <code>display igmp statistics</code> command.</td>
</tr>
</tbody>
</table>
CHAPTER 13: IGMP SNOOPING COMMANDS

See Also

- display igmp mrouter on page 566
- display igmp querier on page 567
- display igmp receiver-table on page 569
- display igmp statistics on page 571

**display igmp mrouter**

Displays the multicast routers in a WX's subnet, on one VLAN or all VLANs. Routers are listed separately for each VLAN, according to the port number through which the wireless LAN switch can reach the router.

**Syntax** — **display igmp mrouter [vlan vlan-id]**

- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, MSS displays the multicast routers in all VLANs.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays the multicast routers in VLAN orange:

```
WX1200# display igmp mrouter vlan orange
Multicast routers for vlan orange
Port Mrouter-IPaddr Mrouter-MAC Type TTL
----- --------------- ----------------- ----- ----- 
1 192.28.7.5 00:01:02:03:04:05 dvmrp 33
```

Table 83 describes the fields in this display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN name. MSS displays information separately for each VLAN.</td>
</tr>
<tr>
<td>IGMP is enabled</td>
<td>IGMP state.</td>
</tr>
<tr>
<td>(disabled)</td>
<td></td>
</tr>
</tbody>
</table>

Table 82  Output for display igmp (continued)
display igmp querier

Shows information about the active multicast querier, on one VLAN or all VLANs. Queriers are listed separately for each VLAN. Each VLAN can have only one querier.

**Syntax** — `display igmp querier [vlan vlan-id]`

- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, MSS displays querier information for all VLANs.

**Defaults** — None.

**Access** — Enabled.

---

### Table 83 Output for display igmp mrouter

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routers for vlan</td>
<td>VLAN containing the multicast routers. Ports are listed separately for each VLAN.</td>
</tr>
<tr>
<td>Port</td>
<td>Number of the physical port through which the WX can reach the router.</td>
</tr>
<tr>
<td>Mrouter-Ipaddr</td>
<td>IP address of the multicast router.</td>
</tr>
<tr>
<td>Mrouter-Mac</td>
<td>MAC address of the multicast router.</td>
</tr>
<tr>
<td>Type</td>
<td>How the WX learned that the port is a multicast router port:</td>
</tr>
<tr>
<td></td>
<td>- <strong>conf</strong> — Static multicast port configured by an administrator</td>
</tr>
<tr>
<td></td>
<td>- <strong>madv</strong> — Multicast advertisement</td>
</tr>
<tr>
<td></td>
<td>- <strong>quer</strong> — IGMP query</td>
</tr>
<tr>
<td></td>
<td>- <strong>dvmrp</strong> — Distance Vector Multicast Routing Protocol (DVMRP)</td>
</tr>
<tr>
<td></td>
<td>- <strong>pimv1</strong> — Protocol Independent Multicast (PIM) version 1</td>
</tr>
<tr>
<td></td>
<td>- <strong>pimv2</strong> — PIM version 2</td>
</tr>
<tr>
<td>TTL</td>
<td>Number of seconds before this entry ages out if unused. For static multicast router entries, the TTL value is <code>undef</code>. Static multicast router entries do not age out.</td>
</tr>
</tbody>
</table>

See Also

- `display igmp mrouter` on page 566
- `set igmp mrouter` on page 575
History — Introduced in MSS Version 3.0.

Examples — The following command displays querier information for VLAN orange:

    WX1200# display igmp querier vlan orange
    Querier for vlan orange
    Port  Querier-IP     Querier-MAC     TTL
    ----  ---------------  ----------------- -----  
    1 193.122.135.178    00:0b:cc:d2:e9:b4  23

The following command shows the information MSS displays when the querier is the WX itself:

    WX1200# display igmp querier vlan default
    Querier for vlan default:
    I am the querier for vlan default, time to next query is 20

The output indicates how many seconds remain before the pseudo-querier on the WX switch broadcasts the next general query report to IP address 224.0.0.1, the multicast all-systems group.

If IGMP snooping does not detect a querier, the output indicates this finding, as shown in the following example:

    WX1200# display igmp querier vlan red
    Querier for vlan red:
    There is no querier present on vlan red

This condition does not necessarily indicate a problem. For example, election of the querier might be in progress.

Table 84 describes the fields in this display. Table 83 on page 567 describes the fields in the display when a querier other than the WX is present.

Table 84  Output for display igmp mrouter

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querier for vlan</td>
<td>VLAN containing the querier. Information is listed separately for each VLAN.</td>
</tr>
<tr>
<td>Querier-IP</td>
<td>IP address of the querier interface.</td>
</tr>
<tr>
<td>Querier-MAC</td>
<td>MAC address of the querier interface.</td>
</tr>
<tr>
<td>TTL</td>
<td>Number of seconds before this entry ages out if the WX does not receive a query message from the querier.</td>
</tr>
</tbody>
</table>
See Also
- set igmp querier on page 581

display igmp receiver-table
Displays the receivers to which a WX forwards multicast traffic. You can display receivers for all VLANs, a single VLAN, or a group or groups identified by group address and network mask.

Syntax — display igmp receiver-table [vlan vlan-id] [group group-ip-addr/mask-length]
- vlan vlan-id — VLAN name or number. If you do not specify a VLAN, MSS displays the multicast receivers on all VLANs.
- group group-ip-addr/mask-length — IP address and subnet mask of a multicast group, in CIDR format (for example, 239.20.20.10/24). If you do not specify a group address, MSS displays the multicast receivers for all groups.

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0.

Examples — The following command displays all multicast receivers in VLAN orange:

WX1200# display igmp receiver-table vlan orange
VLAN: orange
Session | Port | Receiver-IP | Receiver-MAC | TTL
--------|------|-------------|--------------|-----
224.0.0.2 | none | none | none | undef
237.255.255.255 | 5 | 10.10.10.11 | 00:02:04:06:08:0b | 179
237.255.255.255 | 5 | 10.10.10.13 | 00:02:04:06:08:0d | 179
237.255.255.255 | 5 | 10.10.10.14 | 00:02:04:06:08:0e | 179
237.255.255.255 | 5 | 10.10.10.12 | 00:02:04:06:08:0c | 179
237.255.255.255 | 5 | 10.10.10.10 | 00:02:04:06:08:0a | 179
The following command lists all receivers for multicast groups 237.255.255.1 through 237.255.255.255, in all VLANs:

```
WX1200# display igmp receiver-table group 237.255.255.0/24
VLAN: red
Session  Port  Receiver-IP   Receiver-MAC   TTL
---------- -------- --------------- --------------- -----
237.255.255.2  2     10.10.20.19  00:02:04:06:09:0d   112
237.255.255.119 3     10.10.30.31  00:02:04:06:01:0b   112
VLAN: green
Session  Port  Receiver-IP   Receiver-MAC   TTL
---------- -------- --------------- --------------- -----
237.255.255.17 1     10.10.40.41  00:02:06:08:02:0c    12
237.255.255.255 6     10.10.60.61  00:05:09:0c:0a:01   111
```

Table 85 describes the fields in this display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN that contains the multicast receiver ports. Ports are listed separately for each VLAN.</td>
</tr>
<tr>
<td>Session</td>
<td>IP address of the multicast group being received.</td>
</tr>
<tr>
<td>Port</td>
<td>Physical port through which the WX can reach the receiver.</td>
</tr>
<tr>
<td>Receiver-IP</td>
<td>IP address of the receiver.</td>
</tr>
<tr>
<td>Receiver-MAC</td>
<td>MAC address of the receiver.</td>
</tr>
<tr>
<td>TTL</td>
<td>Number of seconds before this entry ages out if the WX does not receive a group membership message from the receiver. For static multicast receiver entries, the TTL value is <code>undef</code>. Static multicast receiver entries do not age out.</td>
</tr>
</tbody>
</table>

See Also

- `set igmp receiver` on page 581
**display igmp statistics**

Shows IGMP statistics.

**Syntax** — `display igmp statistics [vlan vlan-id]`

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS displays IGMP statistics for all VLANs.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command displays IGMP statistics for VLAN `orange`:

```
WX1200# display igmp statistics vlan orange
IGMP statistics for vlan orange:

IGMP message type Received Transmitted Dropped
-------------------- -------- ----------- -------
General-Queries 0 0 0
GS-Queries 0 0 0
Report V1 0 0 0
Report V2 5 1 4
Leave 0 0 0
Mrouter-Adv 0 0 0
Mrouter-Term 0 0 0
Mrouter-Sol 50 101 0
DVMRP 4 4 0
PIM V1 0 0 0
PIM V2 0 0 0

Topology notifications: 0
Packets with unknown IGMP type: 0
Packets with bad length: 0
Packets with bad checksum: 0
Packets dropped: 4
```

Table 86 describes the fields in this display.
### Table 86  Output of display igmp statistics

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP statistics for vlan</td>
<td>VLAN name. Statistics are listed separately for each VLAN.</td>
</tr>
<tr>
<td>IGMP message type</td>
<td>Type of IGMP message:</td>
</tr>
<tr>
<td></td>
<td>- <strong>General-Queries</strong> — General group membership queries sent by the multicast querier (multicast router or pseudo-querier).</td>
</tr>
<tr>
<td></td>
<td>- <strong>GS-Queries</strong> — Group-specific queries sent by the multicast querier to determine whether there are receivers for a specific group.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Report V1</strong> — IGMP version 1 group membership reports sent by clients who want to be receivers for the groups.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Report V2</strong> — IGMP version 2 group membership reports sent by clients who want to be receivers for the groups.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Leave</strong> — IGMP version 2 leave messages sent by clients who want to stop receiving traffic for a group. Leave messages apply only to IGMP version 2.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mrouter-Adv</strong> — Multicast router advertisement packets. A multicast router sends this type of packet to advertise the IP address of the sending interface as a multicast router interface.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mrouter-Term</strong> — Multicast router termination messages. A multicast router sends this type of message when multicast forwarding is disabled on the router interface, the router interface is administratively disabled, or the router itself is gracefully shutdown.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mrouter-Sol</strong> — Multicast router solicitation messages. A multicast client or a WX sends this type of message to immediately solicit multicast router advertisement messages from the multicast routers in the subnet.</td>
</tr>
<tr>
<td></td>
<td>- <strong>DVMRP</strong> — Distance Vector Multicast Routing Protocol (DVMRP) messages. Multicast routers running DVMRP exchange multicast information with these messages.</td>
</tr>
<tr>
<td></td>
<td>- <strong>PIM V1</strong> — Protocol Independent Multicast (PIM) version 1 messages. Multicast routers running PIMv1 exchange multicast information with these messages.</td>
</tr>
<tr>
<td></td>
<td>- <strong>PIM V2</strong> — PIM version 2 messages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received</td>
<td>Number of packets received.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Number of packets transmitted. This number includes both multicast packets originated by the WX and multicast packets received and then forwarded by the WX.</td>
</tr>
<tr>
<td>Dropped</td>
<td>Number of IGMP packets dropped by the WX.</td>
</tr>
</tbody>
</table>
Disables or reenables IGMP snooping on one VLAN or all VLANs on a wireless LAN switch.

**Syntax** — `set igmp {enable | disable} [vlan vlan-id]`

- **enable** — Enables IGMP snooping.
- **disable** — Disables IGMP snooping.
- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, IGMP snooping is disabled or reenabled on all VLANs.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command disables IGMP snooping on VLAN orange:

```shell
WX1200# set igmp disable vlan orange
success: change accepted
```

**See Also**

- **clear igmp statistics** on page 562

---

**Table 86** Output of display igmp statistics (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology notifications</td>
<td>Number of Layer 2 topology change notifications received by the WX.</td>
</tr>
<tr>
<td></td>
<td>In the current software version, the value in this field is always 0.</td>
</tr>
<tr>
<td>Packets with unknown</td>
<td>Number of multicast packets received with an unrecognized multicast type.</td>
</tr>
<tr>
<td>IGMP type</td>
<td></td>
</tr>
<tr>
<td>Packets with bad length</td>
<td>Number of packets with an invalid length.</td>
</tr>
<tr>
<td>Packets with bad IGMP</td>
<td>Number of packets with an invalid IGMP checksum value.</td>
</tr>
<tr>
<td>checksum</td>
<td></td>
</tr>
<tr>
<td>Packets dropped</td>
<td>Number of multicast packets dropped by the WX.</td>
</tr>
</tbody>
</table>

---

**See Also**

- **set igmp rv** on page 582
set igmp lmqi

Changes the IGMP last member query interval timer on one VLAN or all VLANs on a wireless LAN switch.

**Syntax** — `set igmp lmqi tenth-seconds [vlan vlan-id]`

- `lmqi tenth-seconds` — Amount of time (in tenths of a second) that the WX waits for a response to a group-specific query after receiving a leave message for that group, before removing the receiver that sent the leave message from the list of receivers for the group. If there are no more receivers for the group, the WX switch also sends a leave message for the group to multicast routers. You can specify a value from 1 through 65,535.

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

**Defaults** — The default last member query interval is 10 tenths of a second (1 second).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command changes the last member query interval on VLAN *orange* to 5 tenths of a second:

```
WX1200# set igmp lmqi 5 vlan orange
success: change accepted.
```

**See Also**

- `set igmp oqi` on page 577
- `set igmp qi` on page 579
- `set igmp mrouter` on page 575
set igmp mrouter

Adds or removes a port in a WX’s list of ports on which it forwards traffic to multicast routers. Static multicast ports are immediately added to or removed from the list of router ports and do not age out.

Syntax — `set igmp mrouter port port-list {enable | disable}`
- `port port-list` — Port list. MSS adds or removes the specified ports in the list of static multicast router ports.
- `enable` — Adds the port to the list of static multicast router ports.
- `disable` — Removes the port from the list of static multicast router ports.

Defaults — By default, no ports are static multicast router ports.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add MAP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples — The following command adds port 6 as a static multicast router port:
`WX1200# set igmp mrouter port 6 enable`
`success: change accepted.`

The following command removes port 6 from the static multicast router port list:
`WX1200# set igmp mrouter port 6 disable`
`success: change accepted.`

See Also
- `display igmp statistics` on page 571
**set igmp mrsol**  
Enables or disables multicast router solicitation by a WX.

**Syntax** — `set igmp mrsol {enable | disable} [vlan vlan-id]`

- **enable** — Enables multicast router solicitation.
- **disable** — Disables multicast router solicitation.
- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, multicast router solicitation is disabled or enabled on all VLANs.

**Defaults** — Multicast router solicitation is disabled on all VLANs by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command enables multicast router solicitation on VLAN `orange`:

```
WX1200# set igmp mrsol enable vlan orange
success: change accepted
```

**See Also**
- `set igmp mrsol mrsi` on page 576

---

**set igmp mrsol mrsi**  
Changes the interval between multicast router solicitations by a WX on one VLAN or all VLANs.

**Syntax** — `set igmp mrsol mrsi seconds [vlan vlan-id]`

- **seconds** — Number of seconds between multicast router solicitations. You can specify a value from 1 through 65,535.
- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, MSS changes the multicast router solicitation interval for all VLANs.

**Defaults** — The interval between multicast router solicitations is 30 seconds by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
**set igmp oqi**

Changes the IGMP other-querier-present interval timer on one VLAN or all VLANs on a WX.

**Syntax** —  
`set igmp oqi seconds [vlan vlan-id]

- `oqi seconds` — Number of seconds that the WX waits for a general query to arrive before electing itself the querier. You can specify a value from 1 through 65,535.
- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

**Defaults** —  
The default other-querier-present interval is 255 seconds (4.25 minutes).

**Access** —  
Enabled.

**History** —  
Introduced in MSS Version 3.0.

**Usage** —  
A WX cannot become the querier unless the pseudo-querier feature is enabled on the WX switch. When the feature is enabled, the WX becomes the querier for a subnet so long as the WX does not receive a query message from a router with a lower IP address than the IP address of the WX in that subnet. To enable the pseudo-querier feature, use `set igmp querier`.

**Examples** —  
The following command changes the other-querier-present interval on VLAN `orange` to 200 seconds:

```
WX1200# set igmp oqi 200 vlan orange
success: change accepted.
```
**set igmp proxy-report**

Disables or reenables proxy reporting by a WX on one VLAN or all VLANs.

**Syntax** — `set igmp proxy-report {enable | disable}

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, proxy reporting is disabled or reenabled on all VLANs.
- `enable` — Enables proxy reporting.
- `disable` — Disables proxy reporting.

**Defaults** — Proxy reporting is enabled on all VLANs by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Proxy reporting reduces multicast overhead by sending only one membership report for a group to the multicast routers and discarding other membership reports for the same group. If you disable proxy reporting, the WX sends all membership reports to the routers, including multiple reports for the same group.

**Examples** — The following example disables proxy reporting on VLAN orange:

```plaintext
WX1200# set igmp proxy-report disable vlan orange
success: change accepted.
```

**See Also**

- `set igmp lmqi` on page 574
- `set igmp qi` on page 579
- `set igmp qri` on page 580
- `set igmp querier` on page 581
- `set igmp mrouter` on page 575
- `set igmp rv` on page 582
set igmp qi

Changes the IGMP query interval timer on one VLAN or all VLANs on a WX.

Syntax — set igmp qi seconds [vlan vlan-id]

- qi seconds — Number of seconds that elapse between general queries sent by the WX when the WX switch is the querier for the subnet. You can specify a value from 1 through 65,535.
- vlan vlan-id — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default query interval is 125 seconds.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The query interval is applicable only when the WX is querier for the subnet. For the WX switch to become the querier, the pseudo-querier feature must be enabled on the WX and the WX must have the lowest IP address among all the WX switches eligible to become a querier. To enable the pseudo-querier feature, use the set igmp querier command.

Examples — The following command changes the query interval on VLAN orange to 100 seconds:

```
WX1200# set igmp qi 100 vlan orange
success: change accepted.
```

See Also

- set igmp lmqi on page 574
- set igmp oqi on page 577
- set igmp qri on page 580
- set igmp querier on page 581
- set igmp mrouter on page 575
- set igmp rv on page 582
set igmp qri  Changes the IGMP query response interval timer on one VLAN or all VLANs on a WX.

Syntax — set igmp qri tenth-seconds [vlan vlan-id]

- qri tenth-seconds — Amount of time (in tenths of a second) that the WX waits for a receiver to respond to a group-specific query message before removing the receiver from the receiver list for the group. You can specify a value from 1 through 65,535.
- vlan vlan-id — VLAN name or number. If you do not specify a VLAN, the timer change applies to all VLANs.

Defaults — The default query response interval is 100 tenths of a second (10 seconds).

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The query response interval is applicable only when the WX is querier for the subnet. For the WX to become the querier, the pseudo-querier feature must be enabled on the WX and the WX must have the lowest IP address among all the WX switches eligible to become a querier. To enable the pseudo-querier feature, use set igmp querier.

Examples — The following command changes the query response interval on VLAN orange to 50 tenths of a second (5 seconds):

WX1200# set igmp qri 50 vlan orange
success: change accepted.

See Also
- set igmp lmqi on page 574
- set igmp oqi on page 577
- set igmp qi on page 579
- set igmp querier on page 581
- set igmp rv on page 582
### set igmp querier

Enables or disables the IGMP pseudo-querier on a WX, on one VLAN or all VLANs.

**Syntax** — `set igmp querier {enable | disable} [vlan vlan-id]`

- **enable** — Enables the pseudo-querier.
- **disable** — Disables the pseudo-querier.
- **vlan vlan-id** — VLAN name or number. If you do not specify a VLAN, the pseudo-querier is enabled or disabled on all VLANs.

**Defaults** — The pseudo-querier is disabled on all VLANs by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — 3Com recommends that you use the pseudo-querier only when the VLAN contains local multicast traffic sources and no multicast router is servicing the subnet.

**Examples** — The following example enables the pseudo-querier on the orange VLAN:

```bash
WX1200# set igmp querier enable vlan orange
success: change accepted.
```

**See Also**

- `display igmp querier` on page 567

### set igmp receiver

Adds or removes a network port in the list of ports on which a WX forwards traffic to multicast receivers. Static multicast receiver ports are immediately added to or removed from the list of receiver ports and do not age out.

**Syntax** — `set igmp receiver port port-list {enable | disable}`

- **port port-list** — Network port list. MSS adds the specified ports to the list of static multicast receiver ports.
- **enable** — Adds the port to the list of static multicast receiver ports.
- **disable** — Removes the port from the list of static multicast receiver ports.
Defaults — By default, no ports are static multicast receiver ports.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You cannot add MAP access ports or wired authentication ports as static multicast ports. However, MSS can dynamically add these port types to the list of multicast ports based on multicast traffic.

Examples — The following command adds port 7 as a static multicast receiver port:

```
WX1200# set igmp receiver port 7 enable
success: change accepted.
```

The following command removes port 7 from the list of static multicast receiver ports:

```
WX1200# set igmp receiver port 7 disable
success: change accepted.
```

See Also

- `display igmp receiver-table` on page 569

---

**set igmp rv**

Changes the robustness value for one VLAN or all VLANs on a WX. Robustness adjusts the IGMP timers to the amount of traffic loss that occurs on the network.

**Syntax** — `set igmp rv num [vlan vlan-id]`

- `num` — Robustness value. You can specify a value from 2 through 255. Set the robustness value higher to adjust for more traffic loss.

- `vlan vlan-id` — VLAN name or number. If you do not specify a VLAN, MSS changes the robustness value for all VLANs.

Defaults — The default robustness value for all VLANs is 2.

Access — Enabled.

History — Introduced in MSS Version 3.0.
See Also

- `set igmp oqi` on page 577
- `set igmp qi` on page 579
- `set igmp qri` on page 580
CHAPTER 13: IGMP SNOOPING COMMANDS
Use security ACL commands to configure and monitor security access control lists (ACLs). Security ACLs filter packets to restrict or permit network usage by certain users or traffic types, and can assign to packets a class of service (CoS) to define the priority of treatment for packet filtering.

(Security ACLs are different from the location policy on a WX, which helps you locally control user access. For location policy commands, see “AAA Commands” on page 259.)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Security ACLs</td>
<td>set security acl on page 600</td>
</tr>
<tr>
<td></td>
<td>display security acl editbuffer on page 591</td>
</tr>
<tr>
<td></td>
<td>display security acl on page 590</td>
</tr>
<tr>
<td></td>
<td>display security acl info on page 593</td>
</tr>
<tr>
<td></td>
<td>clear security acl on page 586</td>
</tr>
<tr>
<td>Commit Security ACLs</td>
<td>commit security acl on page 589</td>
</tr>
<tr>
<td></td>
<td>rollback security acl on page 599</td>
</tr>
<tr>
<td>Map Security ACLs</td>
<td>set security acl map on page 605</td>
</tr>
<tr>
<td></td>
<td>display security acl map on page 594</td>
</tr>
<tr>
<td></td>
<td>clear security acl map on page 587</td>
</tr>
<tr>
<td>Monitor Security ACLs</td>
<td>display security acl hits on page 592</td>
</tr>
<tr>
<td></td>
<td>set security acl hit-sample-rate on page 607</td>
</tr>
<tr>
<td></td>
<td>display security acl resource-usage on page 595</td>
</tr>
</tbody>
</table>
clear security acl

Clears a specified security ACL, an access control entry (ACE), or all security ACLs, from the edit buffer. When used with the command `commit security acl`, clears the ACE from the running configuration.

**Syntax** — `clear security acl {acl-name | all} [editbuffer-index]`

- `acl-name` — Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.
- `all` — Clears all security ACLs.
- `editbuffer-index` — Number that indicates which access control entry (ACE) in the security ACL to clear. If you do not specify an ACE, all ACEs are cleared from the ACL.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command deletes security ACLs only in the edit buffer. You must use the `commit security acl` command with this command to delete the ACL or ACE from the running configuration and nonvolatile storage.

The `clear security acl` command deletes a security ACL, but does not stop its current filtering function if the ACL is mapped to any virtual LANs (VLANs), ports, or virtual ports, or if the ACL is applied in a Filter-Id attribute to an authenticated user or group of users with current sessions.

**Examples** — The following commands display the current security ACL configuration, `clear acl_133` in the edit buffer, commit the deletion to the running configuration, and redisplay the ACL configuration to display that it no longer contains `acl_133`:
WX4400# display security acl info all
ACL information for all
set security acl ip acl_133 (hits #1 0)
---------------------------------------------------------
1. deny IP source IP 192.168.1.6 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
---------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
---------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits
WX4400# clear security acl acl_133
WX4400# commit security acl acl_133
configuration accepted
WX4400# display security acl info all
ACL information for all
set security acl ip acl_134 (hits #3 0)
---------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
---------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits

See Also
- clear security acl map on page 587
- commit security acl on page 589
- display security acl info on page 593
- set security acl on page 600

---

**clear security acl map**

Deletes the mapping between a security ACL and a virtual LAN (VLAN), one or more physical ports, or a virtual port. Or deletes all ACL maps to VLANs, ports, and virtual ports on a WX switch.

*Security ACLs are applied to users or groups dynamically via the Filter-Id attribute. To delete a security ACL from a user or group in the local WX database, use the command **clear user attr, clear mac-user attr, clear usergroup attr**, or **clear mac-usergroup attr**. To delete a security ACL from a user or group on an external RADIUS server, see the documentation for your RADIUS server.*
**Syntax** — `clear security acl map {acl-name | all} {vlan vlan-id | port port-list [tag tag-value] | ap ap-num} {in | out}

- **acl-name** — Name of an existing security ACL to clear. ACL names start with a letter and are case-insensitive.

- **all** — Removes security ACL mapping from all physical ports, virtual ports, and VLANs on a WX switch.

- **vlan vlan-id** — VLAN name or number. MSS removes the security ACL from the specified VLAN.

- **port port-list** — Port list. MSS removes the security ACL from the specified WX physical port or ports.

- **tag tag-value** — Tag value that identifies a virtual port in a VLAN. Specify a value from 1 through 4095. MSS removes the security ACL from the specified virtual port.

- **ap ap-num** — One or more MAPs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS removes the security ACL from the specified MAPs.

- **in** — Removes the security ACL from traffic coming into the WX switch.

- **out** — Removes the security ACL from traffic going out of the WX switch.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To clear a security ACL map, type the name of the ACL with the VLAN, physical port or ports, virtual port tag, or Distributed MAP and the direction of the packets to stop filtering. This command deletes the ACL mapping, but not the ACL.

**Examples** — To clear the mapping of security ACL acljoe from port 4 for incoming packets, type the following command:

```
WX4400# clear security acl map acljoe port 4 in
clear mapping accepted
```
To clear all physical ports, virtual ports, and VLANs on a WX switch of the ACLs mapped for incoming and outgoing traffic, type the following command:

```plaintext
WX4400# clear security acl map all
success: change accepted.
```

See Also
- `clear security acl` on page 586
- `display security acl map` on page 594
- `set security acl map` on page 605

---

**commit security acl**

Saves a security ACL, or all security ACLs, in the edit buffer to the running configuration and nonvolatile storage on the WX switch. Or, when used with the clear security acl command, `commit security acl` deletes a security ACL, or all security ACLs, from the running configuration and nonvolatile storage.

**Syntax** — `commit security acl {acl-name | all}`

- `acl-name` — Name of an existing security ACL to commit. ACL names must start with a letter and are case-insensitive.
- `all` — Commits all security ACLs in the edit buffer.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Use the `commit security acl` command to save security ACLs into, or delete them from, the permanent configuration. Until you commit the creation or deletion of a security ACL, it is stored in an edit buffer and is not enforced. After you commit a security ACL, it is removed from the edit buffer.

A single `commit security acl all` command commits the creation and/or deletion of whatever `display security acl info all editbuffer` shows to be currently stored in the edit buffer.
Examples — The following commands commit all the security ACLs in the edit buffer to the configuration, display a summary of the committed ACLs, and show that the edit buffer has been cleared:

```
WX4400# commit security acl all
configuration accepted
WX4400# display security acl
ACL table
ACL    Type Class   Mapping
--------- ------- --------
acl_123 IP      Static
acl_124 IP      Static
WX4400# display security acl info all editbuffer
acl editbuffer information for all
```

See Also
- `clear security acl` on page 586
- `display security acl` on page 590
- `display security acl info` on page 593
- `rollback security acl` on page 599
- `set security acl` on page 600

**display security acl**

Displays a summary of the security ACS that are mapped.

Syntax — `display security acl`

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command lists only the ACLs that have been mapped to something (a user, or VLAN, or port, and so on). To list all committed ACLs, use the `display security acl info` command. To list ACLs that have not yet been committed, use the `display security acl editbuffer` command.

Examples — To display a summary of the mapped security ACLs on a WX switch, type the following command:
WX4400# display security acl
ACL table
ACL Type Class Mapping
---------------------------- ---- ------ -------
acl_123 IP Static Port 2 In
acl_133 IP Static Port 4 In
acl_124 IP Static

See Also
- clear security acl on page 586
- display security acl info on page 593
- display security acl editbuffer on page 591
- set security acl on page 600

display security acl editbuffer

Displays a summary of the security ACLs that have not yet been committed to the configuration.

Syntax — display security acl [info all] editbuffer
- info all — Displays the ACEs in each uncommitted ACL. Without this option, only the ACE names are listed.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 1.0.

Examples — To view a summary of the security ACLs in the edit buffer, type the following command:

WX4400# display security acl editbuffer
ACL edit-buffer table
ACL Type Status
---------------------------- ---- ------------------
acl_111 IP Not committed
acl-a IP Not committed
To view details about these uncommitted ACLs, type the following command.

WX4400# display security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl-111 (ACEs 3, add 3, del 0, modified 2)
---------------------------------------------------
1. permit IP source IP 192.168.254.12 0.0.0.0 destination IP any
2. permit IP source IP 192.168.253.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.253.1 0.0.0.255
set security acl ip acl-a (ACEs 1, add 1, del 0, modified 0)
---------------------------------------------------
1. permit SRC source IP 192.168.1.1 0.0.0.0

See Also

- clear security acl on page 586
- commit security acl on page 589
- display security acl on page 590
- display security acl info on page 593
- set security acl on page 600

---

display security acl hits

Displays the number of packets filtered by security ACLs (“hits”) on the WX switch. Each time a packet is filtered by a security ACL, the hit counter increments.

**Syntax** — `display security acl hits`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — For MSS to count hits for a security ACL, you must specify hits in the `set security acl` commands that define ACE rules for the ACL.
Examples — To display the security ACL hits on a WX switch, type the following command:

```
WX4400# display security acl hits
ACL hit-counters
Index Counter ACL-name
----- -------------------- --------
 1    0 acl_2
 2    0 acl_175
 3   916 acl_123
```

See Also

- `set security acl hit-sample-rate` on page 607
- `set security acl` on page 600

**display security acl info**

Displays the contents of a specified security ACL or all security ACLs that are committed — saved in the running configuration and nonvolatile storage — or the contents of security ACLs in the edit buffer before they are committed.

**Syntax** — `display security acl info {acl-name | all} [editbuffer]`

- *acl-name* — Name of an existing security ACL to display. ACL names must start with a letter and are case-insensitive.
- *all* — Displays the contents of all security ACLs.
- *editbuffer* — Displays the contents of the specified security ACL or all security ACLs that are stored in the edit buffer after being created with `set security acl`. If you do not use this parameter, only committed ACLs are shown.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. The *acl-name | all* option is no longer required; `display security acl info` is valid and displays the same information as `security acl info all` in MSS Version 4.1.
Examples — To display the contents of all security ACLs committed on a WX switch, type the following command:

WX4400# display security acl info
ACL information for all
set security acl ip acl_123 (hits #5 462)
---------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
set security acl ip acl_134 (hits #3 0)
---------------------------------------------------------
1. permit IP source IP 192.168.0.1 0.0.0.0 destination IP any enable-hits
set security acl ip acl_135 (hits #2 0)
---------------------------------------------------------
1. deny IP source IP 192.168.1.1 0.0.0.0 destination IP any enable-hits

The following command displays the contents of acl_123 in the edit buffer, including the committed ACE rules 1 and 2 and the uncommitted rule 3:

WX4400# display security acl info acl_123 editbuffer
ACL edit-buffer information for acl_123
set security acl ip acl_123 (ACEs 3, add 3, del 0, modified 0)
---------------------------------------------------------
1. permit IP source IP 192.168.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 192.168.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits

See Also
- clear security acl on page 586
- commit security acl on page 589
- set security acl on page 600

**display security acl map**

Displays the VLANs, ports, and virtual ports on the WX switch to which a security ACL is assigned.

Syntax — `display security acl map acl-name`

- `acl-name` — Name of an existing security ACL for which to show static mapping. ACL names must start with a letter and are case-insensitive.

Defaults — None.
Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command displays the port to which security ACL acl_111 is mapped:

WX4400# display security acl map acl_111
ACL acl_111 is mapped to:
Port 4 in

See Also
- clear security acl map on page 587
- display security acl map on page 594
- set security acl map on page 605

### display security acl resource-usage

Displays statistics about the resources used by security ACL filtering on the WX switch.

Syntax — display security acl resource-usage

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use this command with the help of 3Com to diagnose an ACL resource problem. (To obtain 3Com Technical Support, see “Obtaining Support for Your 3Com Products” on page 787.)
**Examples** — To display security ACL resource usage, type the following command:

```
WX4400# display security acl resource-usage
ACL resources

Classifier tree counters
-------------------------------
  Number of rules : 2
  Number of leaf nodes : 1
  Stored rule count : 2
  Leaf chain count : 1
  Longest leaf chain : 2
  Number of non-leaf nodes : 0
  Uncompressed Rule Count : 2
  Maximum node depth : 1
  Sub-chain count : 0
  PSCBs in primary memory : 0 (max: 512)
  PSCBs in secondary memory : 0 (max: 9728)
  Leaves in primary : 2 (max: 151)
  Leaves in secondary : 0 (max 12096)
  Sum node depth : 1

Information on Network Processor status
---------------------------------------
  Fragmentation control : 0
  UC switchdest : 0

ACL resources
  Port number : 0
  Number of action types : 2
  LUdef in use : 5
  Default action pointer : c8007dc
  L4 global : True
  No rules : False
  Non-IP rules : False
  Root in first : True
  Static default action : False
  No per-user (MAC) mapping : True
  Out mapping : False
  In mapping : True
  No VLAN or PORT mapping : False
  No VPORT mapping : True
```

Table 88 explains the fields in the `display security acl resource-usage` output.
Table 88  Output of display security acl resource-usage

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of rules</td>
<td>Number of security ACEs currently mapped to ports or VLANs.</td>
</tr>
<tr>
<td>Number of leaf nodes</td>
<td>Number of security ACL data entries stored in the rule tree.</td>
</tr>
<tr>
<td>Stored rule count</td>
<td>Number of security ACEs stored in the rule tree.</td>
</tr>
<tr>
<td>Leaf chain count</td>
<td>Number of chained security ACL data entries stored in the rule tree.</td>
</tr>
<tr>
<td>Longest leaf chain</td>
<td>Longest chain of security ACL data entries stored in the rule tree.</td>
</tr>
<tr>
<td>Number of non-leaf nodes</td>
<td>Number of nodes with no data entries stored in the rule tree.</td>
</tr>
<tr>
<td>Uncompressed Rule Count</td>
<td>Number of security ACEs stored in the rule tree, including duplicates—ACEs in ACLs applied to multiple ports, virtual ports, or VLANs.</td>
</tr>
<tr>
<td>Maximum node depth</td>
<td>Number of data elements in the rule tree, from the root to the furthest data entry (leaf).</td>
</tr>
<tr>
<td>Sub-chain count</td>
<td>Sum of action types represented in all security ACL data entries.</td>
</tr>
<tr>
<td>PSCBs in primary memory</td>
<td>Number of pattern search control blocks (PSCBs) stored in primary node memory.</td>
</tr>
<tr>
<td>PSCBs in secondary memory</td>
<td>Number of PSCBs stored in secondary node memory.</td>
</tr>
<tr>
<td>Leaves in primary</td>
<td>Number of security ACL data entries stored in primary leaf memory.</td>
</tr>
<tr>
<td>Leaves in secondary</td>
<td>Number of ACL data entries stored in secondary leaf memory.</td>
</tr>
<tr>
<td>Sum node depth</td>
<td>Total number of security ACL data entries.</td>
</tr>
<tr>
<td>Fragmentation control</td>
<td>Control value for handling fragmented IP packets.</td>
</tr>
<tr>
<td>Note:</td>
<td>The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.</td>
</tr>
<tr>
<td>UC switchdest</td>
<td>Control value for handling fragmented IP packets.</td>
</tr>
<tr>
<td>Note:</td>
<td>The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.</td>
</tr>
<tr>
<td>Port number</td>
<td>Control value for handling fragmented IP packets.</td>
</tr>
<tr>
<td>Note:</td>
<td>The current MSS version filters only the first packet of a fragmented IP packet and passes the remaining fragments.</td>
</tr>
<tr>
<td>Number of action types</td>
<td>Number of actions that can be performed by ACLs. This value is always 2, because ACLs can either permit or deny.</td>
</tr>
</tbody>
</table>
### Table 88  Output of display security acl resource-usage (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LUdef in use</td>
<td>Number of the lookup definition (LUdef) table currently in use for packet handling.</td>
</tr>
<tr>
<td>Default action pointer</td>
<td>Memory address used for packet handling, from which default action data is obtained when necessary.</td>
</tr>
<tr>
<td>L4 global</td>
<td>Security ACL mapping on the WX switch:</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong> — Security ACLs are mapped.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> — No security ACLs are mapped.</td>
</tr>
<tr>
<td>No rules</td>
<td>Security ACE rule mapping on the WX switch:</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong> — No security ACEs are mapped.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> — Security ACEs are mapped.</td>
</tr>
<tr>
<td>Non-IP rules</td>
<td>Non-IP security ACE mapping on the WX switch:</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong> — Non-IP security ACEs are mapped.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> — Only IP security ACEs are mapped.</td>
</tr>
<tr>
<td>Note:</td>
<td>The current MSS version supports security ACEs for IP only.</td>
</tr>
<tr>
<td>Root in first</td>
<td>Leaf buffer allocation:</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong> — Enough primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> — Insufficient primary leaf buffers are allocated in nonvolatile memory to accommodate all leaves.</td>
</tr>
<tr>
<td>Static default action</td>
<td>Definition of a default action:</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong> — A default action types is defined.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> — No default action type is defined.</td>
</tr>
<tr>
<td>No per-user (MAC) mapping</td>
<td>Per-user application of a security ACL with the Filter-Id attribute, on the WX switch:</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong> — No security ACLs are applied to users.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> — Security ACLs are applied to users.</td>
</tr>
<tr>
<td>Out mapping</td>
<td>Application of security ACLs to outgoing traffic on the WX switch:</td>
</tr>
<tr>
<td></td>
<td><strong>True</strong> — Security ACLs are mapped to outgoing traffic.</td>
</tr>
<tr>
<td></td>
<td><strong>False</strong> — No security ACLs are mapped to outgoing traffic.</td>
</tr>
</tbody>
</table>
rollback security acl

Clears changes made to the security ACL edit buffer since it was last saved. The ACL is rolled back to its state after the last **commit security acl** command was entered. All uncommitted ACLs in the edit buffer are cleared.

**Syntax** — rollback security acl {acl-name | all}

- **acl-name** — Name of an existing security ACL to roll back. ACL names must start with a letter and are case-insensitive.
- **all** — Rolls back all security ACLs in the edit buffer, clearing all uncommitted ACEs.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
Examples — The following commands show the edit buffer before a rollback, clear any changes in the edit buffer to security acl_122, and show the edit buffer after the rollback:

WX4400# display security acl info all editbuffer
ACL edit-buffer information for all
set security acl ip acl_122 (ACEs 3, add 3, del 0, modified 0)

1. permit IP source IP 20.0.1.11 0.0.0.255 destination IP any enable-hits
2. deny IP source IP 20.0.2.11 0.0.0.0 destination IP any
3. deny SRC source IP 192.168.1.234 255.255.255.255 enable-hits
WX4400# rollback security acl acl_122
WX4400# display security acl info all editbuffer
ACL edit-buffer information for all

See Also
- display security acl on page 590

set security acl
In the edit buffer, creates a security access control list (ACL), adds one access control entry (ACE) to a security ACL, and/or reorders ACEs in the ACL. The ACEs in an ACL filter IP packets by source IP address, a Layer 4 protocol, or IP, ICMP, TCP, or UDP packet information.

By source address

Syntax — set security acl ip acl-name {permit [cos cos] | deny} source-ip-addr mask [before editbuffer-index | modify editbuffer-index] [hits]

By Layer 4 protocol

Syntax — set security acl ip acl-name {permit [cos cos] | deny} protocol-number {source-ip-addr mask destination-ip-addr mask} [precedence precedence] [tos tos] [before editbuffer-index | modify editbuffer-index] [hits]

By IP packets

Syntax — set security acl ip acl-name {permit [cos cos] | deny} ip {source-ip-addr mask destination-ip-addr mask} [precedence precedence] [tos tos] [before editbuffer-index | modify editbuffer-index] [hits]
By ICMP packets

**Syntax** — set security acl ip acl-name {permit [cos cos] | deny} icmp {source-ip-addr mask destination-ip-addr mask [type icmp-type] [code icmp-code] [precedence precedence] [tos tos] [before editbuffer-index | modify editbuffer-index] [hits]

By TCP packets

**Syntax** — set security acl ip acl-name {permit [cos cos] | deny} tcp {source-ip-addr mask [operator port [port2]] destination-ip-addr mask [operator port [port2]]} [precedence precedence] [tos tos] [established] [before editbuffer-index | modify editbuffer-index] [hits]

By UDP packets

**Syntax** — set security acl ip acl-name {permit [cos cos] | deny} udp {source-ip-addr mask [operator port [port2]] destination-ip-addr mask [operator port [port2]]} [precedence precedence] [tos tos] [before editbuffer-index | modify editbuffer-index] [hits]

- **acl-name** — Security ACL name. ACL names must be unique within the WX switch, must start with a letter, and are case-insensitive. Specify an ACL name of up to 32 of the following characters:
  - Letters a through z and A through Z
  - Numbers 0 through 9
  - Hyphen (-), underscore (_), and period (.)

  3Com recommends that you do not use the same name with different capitalizations for ACLs. For example, do not configure two separate ACLs with the names acl_123 and ACL_123.

  **In an ACL name, do not include the term all, default-action, map, help, or editbuffer.**

- **permit** — Allows traffic that matches the conditions in the ACE.
- **cos cos** — For permitted packets, a class-of-service (CoS) level for packet handling. Specify a value from 0 through 7:
  - 1 or 2 — Background. Packets are queued in MAP forwarding queue 4.
• 0 or 3—Best effort. Packets are queued in MAP forwarding queue 3.
• 4 or 5—Video. Packets are queued in MAP forwarding queue 2. Use CoS level 4 or 5 for voice over IP (VoIP) packets other than SpectraLink Voice Priority (SVP).
• 6 or 7—Voice. Packets are queued in MAP forwarding queue 1. In MSS Version 3.0, use 6 or 7 only for VoIP phones that use SVP, not for other types of traffic.

• **deny** — Blocks traffic that matches the conditions in the ACE.

• **protocol** — IP protocol by which to filter packets:
  • ip
  • tcp
  • udp
  • icmp
  • A protocol number between 0 and 255. (For a complete list of IP protocol names and numbers, see www.iana.org/assignments/protocol-numbers.)

• **source-ip-addr mask** — IP address and wildcard mask of the network or host from which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see "Wildcard Masks" on page 78.

• **operator port [port2]** — Operand and port number(s) for matching TCP or UDP packets to the number of the source or destination port on source-ip-addr or destination-ip-addr. Specify one of the following operands and the associated port:
  • eq — Packets are filtered for only port number.
  • gt — Packets are filtered for all ports that are greater than port number.
  • lt — Packets are filtered for all ports that are less than port number.
  • neq — Packets are filtered for all ports except port number.
  • range — Packets are filtered for ports in the range between port and port2. To specify a port range, enter two port numbers. Enter the lower port number first, followed by the higher port number.
(For a complete list of TCP and UDP port numbers, see www.iana.org/assignments/port-numbers.)

- **destination-ip-addr mask** — IP address and wildcard mask of the network or host to which the packet is being sent. Specify both address and mask in dotted decimal notation. For more information, see “Wildcard Masks” on page 78.

- **type icmp-type** — Filters ICMP messages by type. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)

- **code icmp-code** — For ICMP messages filtered by type, additionally filters ICMP messages by code. Specify a value from 0 through 255. (For a list of ICMP message type and code numbers, see www.iana.org/assignments/icmp-parameters.)

- **precedence precedence** — Filters packets by precedence level. Specify a value from 0 through 7:
  - 0 — routine precedence
  - 1 — priority precedence
  - 2 — immediate precedence
  - 3 — flash precedence
  - 4 — flash override precedence
  - 5 — critical precedence
  - 6 — internetwork control precedence
  - 7 — network control precedence

- **tos tos** — Filters packets by type of service (TOS) level. Specify one of the following values, or any sum of these values up to 15. For example, a tos value of 9 filters packets with the TOS levels minimum delay (8) and minimum monetary cost (1).
  - 8 — minimum delay
  - 4 — maximum throughput
  - 2 — maximum reliability
  - 1 — minimum monetary cost
  - 0 — normal

- **established** — For TCP packets only, applies the ACE only to established TCP sessions and not to new TCP sessions.
before editbuffer-index — Inserts the new ACE in front of another ACE in the security ACL. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use 
\texttt{display security acl editbuffer}.)

modify editbuffer-index — Replaces an ACE in the security ACL with the new ACE. Specify the number of the existing ACE in the edit buffer. Index numbers start at 1. (To display the edit buffer, use 
\texttt{display security acl editbuffer}.)

hits — Tracks the number of packets that are filtered based on a security ACL, for all mappings.

Defaults — Permitted packets are assigned to class-of-service (CoS) class 0 by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The WX switch does not apply security ACLs until you activate them with the \texttt{commit security acl} command and map them to a VLAN, port, or virtual port, or to a user. If the WX switch is reset or restarted, any ACLs in the edit buffer are lost.

You cannot perform ACL functions that include permitting, denying, or marking with a Class of Service (CoS) level on packets with a multicast or broadcast destination address.

The order of security ACEs in a security ACL is important. Once an ACL is active, its ACEs are checked according to their order in the ACL. If an ACE criterion is met, its action takes place and any ACEs that follow are ignored.

ACEs are listed in the order in which you create them, unless you move them. To position security ACEs within a security ACL, use \texttt{before editbuffer-index} and \texttt{modify editbuffer-index}.

Examples — The following command adds an ACE to security acl_123 that permits packets from IP address 192.168.1.11/24 and counts the hits:

\texttt{WX4400# set security acl ip acl_123 permit 192.168.1.11 0.0.0.255 hits}
The following command adds an ACE to `acl_123` that denies packets from IP address 192.168.2.11:

```
WX4400# set security acl ip acl_123 deny 192.168.2.11 0.0.0.0
```

The following command creates `acl_125` by defining an ACE that denies TCP packets from source IP address 192.168.0.1 to destination IP address 192.168.0.2 for established sessions only, and counts the hits:

```
WX4400# set security acl ip acl_125 deny tcp 192.168.0.1 0.0.0.0 192.168.0.2 0.0.0.0 established hits
```

The following command adds an ACE to `acl_125` that denies TCP packets from source IP address 192.168.1.1 to destination IP address 192.168.1.2, on destination port 80 only, and counts the hits:

```
WX4400# set security acl ip acl_125 deny tcp 192.168.1.1 0.0.0.0 192.168.1.2 0.0.0.0 eq 80 hits
```

Finally, the following command commits the security ACLs in the edit buffer to the configuration:

```
WX4400# commit security acl all
configuration accepted
```

**See Also**

- `clear security acl` on page 586
- `commit security acl` on page 589
- `display security acl` on page 590

---

**set security acl map**

Assigns a committed security ACL to a VLAN, physical port or ports, virtual port, or Distributed MAP on the WX switch.

*To assign a security ACL to a user or group in the local WX database, use the command `set user attr`, `set mac-user attr`, `set usergroup attr`, or `set mac-usergroup attr` with the Filter-Id attribute. To assign a security ACL to a user or group with Filter-Id on a RADIUS server, see the documentation for your RADIUS server.*
Syntax — set security acl map acl-name \{vlan vlan-id | port port-list [tag tag-list] | ap ap-num\} \{in | out\}

- acl-name — Name of an existing security ACL to map. ACL names start with a letter and are case-insensitive.
- vlan vlan-id — VLAN name or number. MSS assigns the security ACL to the specified VLAN.
- port port-list — Port list. MSS assigns the security ACL to the specified physical WX port or ports.
- tag tag-list — One or more values that identify a virtual port in a VLAN. Specify a single tag value from 1 through 4095. Or specify a comma-separated list of values, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified virtual port or ports.
- ap ap-num — One or more MAPs, based on their connection IDs. Specify a single connection ID, or specify a comma-separated list of connection IDs, a hyphen-separated range, or any combination, with no spaces. MSS assigns the security ACL to the specified MAPs.
- in — Assigns the security ACL to traffic coming into the WX switch.
- out — Assigns the security ACL to traffic coming from the WX switch.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Before you can map a security ACL, you must use the commit security acl command to save the ACL in the running configuration and nonvolatile storage.

For best results, map only one input security ACL and one output security ACL to each VLAN, physical port, virtual port, or Distributed MAP to filter a flow of packets. If more than one security ACL filters the same traffic, MSS applies only the first ACL match and ignores any other matches.

Examples — The following command maps security ACL acl_133 to port 4 for incoming packets:

WX4400 set security acl map acl_133 port 4 in
success: change accepted.
**set security acl hit-sample-rate**

Specifies the time interval, in seconds, at which the packet counter for each security ACL is sampled for display. The counter counts the number of packets filtered by the security ACL — or “hits.”

**Syntax** — `set security acl hit-sample-rate` *seconds*

- *seconds* — Number of seconds between samples. A sample rate of 0 (zero) disables the sample process.

**Defaults** — By default, the hits are not sampled.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Syntax changed from `hit-sample-rate seconds` to `set security acl hit-sample-rate seconds`, to allow the command to be saved in the configuration file.

**Usage** — To view counter results for a particular ACL, use the `display security acl info acl-name` command. To view the hits for all security ACLs, use the `display security acl hits` command.

---

**See Also**

- `clear security acl map` on page 587
- `commit security acl` on page 589
- `set mac-user attr` on page 309
- `set mac-usergroup attr` on page 315
- `set security acl` on page 600
- `set user attr` on page 321
- `set usergroup` on page 323
- `display security acl map` on page 594
Examples — The first command sets MSS to sample ACL hits every 15 seconds. The second and third commands display the results. The results show that 916 packets matching security acl_153 were sent since the ACL was mapped.

WX4400# set security acl hit-sample-rate 15
WX4400# display security acl info acl_153
ACL information for acl_153
set security acl ip acl_153 (hits #3 916)
---------------------------------------------------------
1. permit IP source IP 20.1.1.1 0.0.0.0 destination IP any enable-hits

WX4400# display security acl hits
ACL hit counters
Index Counter ACL-name
----- --------------- ----------
1 0 acl_2
2 0 acl_175
3 916 acl_153

See Also
- display security acl hits on page 592
- display security acl info on page 593
A digital certificate is a form of electronic identification for computers. The WX requires digital certificates to authenticate its communications to 3WXM and Web Manager, to WebAAA clients, and to Extensible Authentication Protocol (EAP) clients for which the WX performs all EAP processing. Certificates can be generated on the WX or obtained from a certificate authority (CA). Keys contained within the certificates allow the WX, its servers, and its wireless clients to exchange information secured by encryption.

If the switch does not already have certificates, MSS automatically generates the missing ones the first time you boot using MSS Version 4.2 or later. You do not need to install certificates unless you want to replace the ones automatically generated by MSS. (For more information, see the “Certificates Automatically Generated by MSS” section in the “Managing Keys and Certificates” chapter of the Wireless LAN Switch and Controller Configuration Guide.)

Before installing a new certificate, verify with the display timedate and display timezone commands that the WX is set to the correct date, time, and time zone. Otherwise, certificates might not be installed correctly.
This chapter presents cryptography commands alphabetically. Use Table 89 to locate commands in this chapter based on their use.

**Table 89  Cryptography Commands by Usage**

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Keys</td>
<td>crypto generate key on page 613</td>
</tr>
<tr>
<td></td>
<td>display crypto key ssh on page 624</td>
</tr>
<tr>
<td></td>
<td>display crypto key domain on page 624</td>
</tr>
<tr>
<td>PKCS #7 Certificates</td>
<td>crypto generate request on page 614</td>
</tr>
<tr>
<td></td>
<td>crypto ca-certificate on page 610</td>
</tr>
<tr>
<td></td>
<td>display crypto ca-certificate on page 621</td>
</tr>
<tr>
<td></td>
<td>crypto certificate on page 612</td>
</tr>
<tr>
<td></td>
<td>display crypto certificate on page 622</td>
</tr>
<tr>
<td>PKCS #12 Certificate</td>
<td>crypto otp on page 618</td>
</tr>
<tr>
<td></td>
<td>crypto pkcs12 on page 620</td>
</tr>
<tr>
<td>Self-Signed Certificate</td>
<td>crypto generate self-signed on page 616</td>
</tr>
</tbody>
</table>

**crypto ca-certificate**

Installs a certificate authority’s own PKCS #7 certificate into the WX certificate and key storage area.

**Syntax** — crypto ca-certificate {admin | eap | web} PEM-formatted certificate

- **admin** — Stores the certificate authority's certificate that signed the administrative certificate for the WX switch.
  
  The administrative certificate authenticates the WX to 3Com wireless switch manager (3XWM) or Web View.

- **eap** — Stores the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the WX switch.
  
  The EAP certificate authenticates the WX to 802.1X supplicants (clients).

- **web** — Stores the certificate authority's certificate that signed the WebAAA certificate for the WX switch.
  
  The Web certificate authenticates the WX to clients who use WebAAA.
crypto ca-certificate

- **PEM-formatted certificate** — ASCII text representation of the certificate authority PKCS #7 certificate, consisting of up to 5120 characters that you have obtained from the certificate authority.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

**Usage** — The Privacy-Enhanced Mail protocol (PEM) format is used for representing a PKCS #7 certificate in ASCII text. PEM uses base64 encoding to convert the certificate to ASCII text, then puts the encoded text between the following delimiters:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

To use this command, you must already have obtained a copy of the certificate authority’s certificate as a PKCS #7 object file. Then do the following:

1. Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
2. Enter the `crypto ca-certificate` command on the CLI command line.
3. When MSS prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

**Examples** — The following command adds the certificate authority’s certificate to WX certificate and key storage:

```
WX4400# crypto ca-certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIDwDCCA2qgAwIBAgIQL2jvuu4P05FAQCyewU3ojANBgkqhkiG9w0BAQUFADCB
mzerMC1aweVQQTToeowi\wpoer0QWNFNkj90044mbdr11277SWQ8G7DiwYUtrqoQplKJvxz
....
Lm8wnVYxP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

**See Also**
- `display crypto ca-certificate` on page 621
**crypto certificate**

Installs one of the WX switch’s PKCS #7 certificates into the certificate and key storage area on the WX switch. The certificate, which is issued and signed by a certificate authority, authenticates the WX switch either to 3WXM or Web Manager, or to 802.1X supplicants (clients).

**Syntax** — `crypto certificate {admin | eap | web} PEM-formatted certificate`

- **admin** — Stores the certificate authority’s administrative certificate, which authenticates the WX switch to 3WXM or Web Manager.
- **eap** — Stores the certificate authority’s Extensible Authentication Protocol (EAP) certificate, which authenticates the WX switch to 802.1X supplicants (clients).
- **web** — Stores the certificate authority’s WebAAA certificate, which authenticates the WX to clients who use WebAAA.
- **PEM-formatted certificate** — ASCII text representation of the PKCS #7 certificate, consisting of up to 5120 characters, that you have obtained from the certificate authority.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

**Usage** — To use this command, you must already have generated a certificate request with the `crypto generate request` command, sent the request to the certificate authority, and obtained a signed copy of the WX switch certificate as a PKCS #7 object file. Then do the following:

1. Open the PKCS #7 object file with an ASCII text editor such as Notepad or vi.
2. Enter the `crypto certificate` command on the CLI command line.
3. When MSS prompts you for the PEM-formatted certificate, paste the PKCS #7 object file onto the command line.

The WX switch verifies the validity of the public key associated with this certificate before installing it, to prevent a mismatch between the WX switch’s private key and the public key in the installed certificate.
Examples — The following command installs a certificate:

```
WX4400# crypto certificate admin
Enter PEM-encoded certificate
-----BEGIN CERTIFICATE-----
MIIBdTCP3wIBADB2MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExGjAYBgNVBAMU
EXR1Y2lwJzQRycHouY29tMIGfMAOGCSqGSIb3DQECBAQAA4GNADCBiQKBgC4 ....
2L8Q9tG2As84Yl5m8vmyVY>xP56M;CUAm908C2foYgOY40=
-----END CERTIFICATE-----
```

See Also
- `crypto generate request` on page 614
- `crypto generate self-signed` on page 616

crypto generate key

Generates an RSA public-private encryption key pair that is required for a Certificate Signing Request (CSR) or a self-signed certificate. For SSH, the command generates an SSH authentication key.

**Syntax** — `crypto generate key {admin | domain | eap | ssh | web} {128 | 512 | 1024 | 2048}`

- **admin** — Generates an administrative key pair for authenticating the WX switch to 3WXM or Web Manager.
- **domain** — Generates a key pair for securing the management traffic between WX switches.
- **eap** — Generates an EAP key pair for authenticating the WX switch to 802.1X supplicants (clients).
- **ssh** — Generates a key pair for authenticating the WX switch to Secure Shell (SSH) clients.
- **web** — Generates an administrative key pair for authenticating the WX switch to WebAAA clients.

- **512 | 1024 | 2048** — Length of the key pair in bits.
  The minimum key size for SSH is 1024.

**Defaults** — None.

**Access** — Enabled.
CHAPTER 15: CRYPTOGRAPHY COMMANDS


Usage — You can overwrite a key by generating another key of the same type.

SSH requires an SSH authentication key, but you can allow MSS to generate it automatically. The first time an SSH client attempts to access the SSH server on a WX switch, the switch automatically generates a 1024-byte SSH key. If you want to use a 2048-byte key instead, use the crypto generate key ssh 2048 command to generate one.

Examples — To generate an administrative key for use with 3WXM, type the following command:

WX4400# crypto generate key admin 1024
key pair generated

See Also
* display crypto key ssh on page 624

crypto generate request

Generates a Certificate Signing Request (CSR). This command outputs a PEM-formatted PKCS #10 text string that you can cut and paste to another location for delivery to a certificate authority.

This command generates either an administrative CSR for use with 3WXM and Web View, or an EAP CSR for use with 802.1X clients.

Syntax — crypto generate request {admin | eap | web}

- admin — Generates a request for an administrative certificate to authenticate the WX switch to 3WXM or Web Manager.
- eap — Generates a request for an EAP certificate to authenticate the WX switch to 802.1X supplicants (clients).
- web — Generates a request for a WebAAA certificate to authenticate the WX switch to WebAAA clients.

After you type the command, you are prompted for the following variables:

- Country Name string — (Optional) Specify the abbreviation for the country in which the WX switch is operating, in 2 alphanumeric characters with no spaces.
- **State Name** *string* — (Optional) Specify the name of the state, in up to 64 alphanumeric characters. Spaces are allowed.
- **Locality Name** *string* — (Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.
- **Organizational Name** *string* — (Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.
- **Organizational Unit** *string* — (Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.
- **Common Name** *string* — Specify a unique name for the WX switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.
- **Email Address** *string* — (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.
- **Unstructured Name** *string* — (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. The `webaaa` option renamed to `web` in MSS Version 4.1. Maximum string length for State Name increased from two to 64 alphanumeric characters.

**Usage** — To use this command, you must already have generated a public-private encryption key pair with the `crypto generate key` command.

Enter `crypto generate request admin`, `crypto generate request eap`, or `crypto generate request web` and press Enter. When you are prompted, type the identifying values in the fields, or press Enter if the field is optional. You must enter a common name for the WX switch.

This command outputs a PKCS #10 text string in Privacy-Enhanced Mail protocol (PEM) format that you paste to another location for submission to the certificate authority. You then send the request to the certificate authority to obtain a signed copy of the WX switch certificate as a PKCS #7 object file.
Examples — To request an administrative certificate from a certificate authority, type the following command:

WX4400# crypto generate request admin
Country Name: US
State Name: CA
Locality Name: Pleasanton
Organizational Name: MyCorp
Organizational Unit: ENG
Common Name: ENG
Email Address: admin@example.com
Unstructured Name: admin
CSR for admin is
-----BEGIN CERTIFICATE REQUEST-----
MIIBuzCCASQAwezELMAkGA1UEBhMCdXMxCzAJBgNVBAgTAmNhMQswCQYDVQQH
EwJjYTELMAkGA1UEChMCY2ExCzAJBgNVBAsTAmNhMQswCQYDVQQDEwJjYTEYMBYG
CSqGSIb3DQEJARYJY2FAY2EuY29tMRkwFwYDV2VuZDIEY2FAY2EuY29tMEcGCCsG
S0ABAG51MWYwcm9wbGVhc2libmZrdWkNMDkwNjBAMDAwMDAwMRYw
-----END CERTIFICATE REQUEST-----

See Also

- crypto certificate on page 612
- crypto generate key on page 613

crypto generate self-signed

Generates a self-signed certificate for either an administrative certificate for use with 3WXM or an EAP certificate for use with 802.1X wireless users.

Syntax — crypto generate self-signed {admin | eap | web}

- admin — Generates an administrative certificate to authenticate the WX switch to 3WXM or Web Manager.
- eap — Generates an EAP certificate to authenticate the WX switch to 802.1X supplicants (clients).
- web — Generates a WebAAA certificate to authenticate the WX switch to WebAAA clients.
After you type the command, you are prompted for the following variables:

- **Country Name string** — (Optional) Specify the abbreviation for the country in which the WX switch is operating, in 2 alphanumeric characters with no spaces.

- **State Name string** — (Optional) Specify the abbreviation for the name of the state, in 2 alphanumeric characters with no spaces.

- **Locality Name string** — (Optional) Specify the name of the locality, in up to 80 alphanumeric characters with no spaces.

- **Organizational Name string** — (Optional) Specify the name of the organization, in up to 80 alphanumeric characters with no spaces.

- **Organizational Unit string** — (Optional) Specify the name of the organizational unit, in up to 80 alphanumeric characters with no spaces.

- **Common Name string** — Specify a unique name for the WX switch, in up to 80 alphanumeric characters with no spaces. Use a fully qualified name if such names are supported on your network. This field is required.

  **Note:** If you are generating a WebAAA (web) certificate, use a common name that looks like a domain name (two or more strings connected by dots, with no spaces). For example, use common.name instead of common name. The string is not required to be an actual domain name. It simply needs to be formatted like one.

- **Email Address string** — (Optional) Specify your email address, in up to 80 alphanumeric characters with no spaces.

- **Unstructured Name string** — (Optional) Specify any name, in up to 80 alphanumeric characters with no spaces.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

**Usage** — To use this command, you must already have generated a public-private encryption key pair with the `crypto generate key` command.
To generate a self-signed administrative certificate, type the following command:

```
WX4400# crypto generate self-signed admin
Country Name: 
State Name: 
Locality Name: 
Organizational Name: 
Organizational Unit: 
Common Name: wx1@example.com
Email Address: 
Unstructured Name: 
success: self-signed cert for admin generated
```

See Also
- crypto certificate on page 612
- crypto generate key on page 613

---

crypto otp

Sets a one-time password (OTP) for use with the crypto pkcs12 command.

**Syntax**
```
crypto otp {admin | eap | web} one-time-password
```

- **admin** — Creates a one-time password for installing a PKCS #12 object file for an administrative certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to 3WXM or Web Manager.
- **eap** — Creates a one-time password for installing a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to 802.1X supplicants (clients).
- **web** — Creates a one-time password for installing a PKCS #12 object file for a WebAAA certificate and key pair—and optionally the certificate authority's own certificate—to authenticate the WX switch to WebAAA clients.
- **one-time-password** — Password of at least 1 alphanumeric character, with no spaces, for clients other than Microsoft Windows clients. The password must be the same as the password protecting the PKCS #12 object file.
**Note:** On an WX switch that handles communications to and from Microsoft Windows clients, use a one-time password of 31 characters or fewer.

The following characters *cannot* be used as part of the one-time password of a PKCS #12 file:

- Quotation marks (" ")
- Question mark (?)
- Ampersand (&)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

**Usage** — The password allows the public-private key pair and certificate to be installed together from the same PKCS #12 object file. MSS erases the one-time password after processing the **crypto pkcs12** command or when you reboot the WX switch.

3Com recommends that you create a password that is memorable to you but is not subject to easy guesses or a dictionary attack. For best results, create a password of alphanumeric uppercase and lowercase characters.

**Examples** — The following command creates the one-time password `hap9iN#ss` for installing an EAP certificate and key pair:

```bash
WX4400# crypto generate otp eap hap9iN#ss
OTP set
```

**See Also**

- crypto **pkcs12** on page 620
**crypto pkcs12**

Unpacks a PKCS #12 object file into the certificate and key storage area on the WX switch. This object file contains a public-private key pair, an WX certificate signed by a certificate authority, and the certificate authority's certificate.

**Syntax**

```
crypto pkcs12 {admin | eap | web} file-location-url
```

- **admin** — Unpacks a PKCS #12 object file for an administrative certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to 3WXM or Web Manager.
- **eap** — Unpacks a PKCS #12 object file for an EAP certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to 802.1X supplicants (clients).
- **web** — Unpacks a PKCS #12 object file for a WebAAA certificate and key pair — and optionally the certificate authority's own certificate — for authenticating the WX switch to WebAAA clients.
- **file-location-url** — Location of the PKCS #12 object file to be installed. Specify a location of between 1 and 128 alphanumeric characters, with no spaces.

**Defaults** — The password you enter with the crypto otp command must be the same as the one protecting the PKCS #12 file.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. **Webaaa** option renamed to **web** in MSS Version 4.1.

**Usage** — To use this command, you must have already created a one-time password with the crypto otp command.

You must also have the PKCS #12 object file available. You can download a PKCS #12 object file via TFTP from a remote location to the local nonvolatile storage system on the WX switch.
**Examples** — The following commands copy a PKCS #12 object file for an EAP certificate and key pair—and optionally the certificate authority's own certificate—from a TFTP server to nonvolatile storage on the WX switch, create the one-time password `hap9iN#ss`, and unpack the PKCS #12 file:

```
WX4400# copy tftp://192.168.253.1/2048full.p12 2048full.p12
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
WX4400# crypto otp eap hap9iN#ss
OTP set
WX4400# crypto pkcs12 eap 2048full.p12
Unwrapped from PKCS12 file:
  keypair
  device certificate
  CA certificate
```

**See Also**

- `crypto otp` on page 618

---

**display crypto ca-certificate**

Displays information about the certificate authority's PEM-encoded PKCS #7 certificate.

**Syntax** — `display crypto ca-certificate {admin | eap | web}`

- `admin` — Displays information about the certificate authority's certificate that signed the administrative certificate for the WX switch. The administrative certificate authenticates the WX to 3WXM or WebView.

- `eap` — Displays information about the certificate authority's certificate that signed the Extensible Authentication Protocol (EAP) certificate for the WX switch. The EAP certificate authenticates the WX switch to 802.1X supplicants (clients).

- `web` — Displays information about the certificate authority's certificate that signed the WebAAA certificate for the WX switch. The WebAAA certificate authenticates the WX switch to WebAAA clients.

**Defaults** — None.
**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. **Webaaa** option renamed to web in MSS Version 4.1.

**Examples** — To display information about the certificate of a certificate authority, type the following command:

```
WX4400# display crypto ca-certificate
```

Table 90 describes the fields in the display.

### Table 90 display crypto ca-certificate Output

<table>
<thead>
<tr>
<th><strong>Fields</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version of the X.509 certificate.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>A unique identifier for the certificate or signature.</td>
</tr>
<tr>
<td>Subject</td>
<td>Name of the certificate owner.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Algorithm that created the signature, such as RSA MD5 or RSA SHA.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Certificate authority that issued the certificate or signature.</td>
</tr>
<tr>
<td>Validity</td>
<td>Time period for which the certificate is valid.</td>
</tr>
</tbody>
</table>

**See Also**

- crypto ca-certificate on page 610
- display crypto certificate on page 622

**display crypto certificate** Displays information about one of the cryptographic certificates installed on the WX switch.

**Syntax** — `display crypto certificate {admin | eap | web}`

- **admin** — Displays information about the administrative certificate that authenticates the WX switch to 3WXM or Web Manager.
- **eap** — Displays information about the EAP certificate that authenticates the WX switch to 802.1X supplicants (clients).
- **web** — Displays information about the WebAAA certificate that authenticates the WX switch to WebAAA clients.
Defaults — None.

Access — Enabled.


Usage — You must have generated a self-signed certificate or obtained a certificate from a certificate authority before displaying information about the certificate.

Examples — To display information about a cryptographic certificate, type the following command:

    WX4400# display crypto certificate eap

Table 91 describes the fields of the display.

### Table 91  crypto certificate Output

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version of the X.509 certificate.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>A unique identifier for the certificate or signature.</td>
</tr>
<tr>
<td>Subject</td>
<td>Name of the certificate owner.</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>Algorithm that created the signature, such as RSA MD5 or RSA SHA.</td>
</tr>
<tr>
<td>Issuer</td>
<td>Certificate authority that issued the certificate or signature.</td>
</tr>
<tr>
<td>Validity</td>
<td>Time period for which the certificate is valid.</td>
</tr>
</tbody>
</table>

See Also crypto generate key on page 613
### display crypto key domain

Displays domain key information.

**Syntax** — `display crypto key domain`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To display domain key information, type the following command:

```
WX4400# display crypto key domain
```

**See Also** `crypto generate key` on page 613

### display crypto key ssh

Displays SSH authentication key information. This command displays the checksum (also called a *fingerprint*) of the public SSH authentication key. When you connect to the WX switch with an SSH client, you can compare the SSH key checksum displayed by the WX switch with the one displayed by the client to verify that you really are connected to the WX switch and not another device. Generally, SSH clients remember the encryption key after the first connection, so you need to check the key only once.

**Syntax** — `display crypto key ssh`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To display SSH key information, type the following command:

```
WX4400# display crypto key ssh
```

**See Also** `crypto generate key` on page 613
RADIUS AND SERVER GROUP COMMANDS

Use RADIUS commands to set up communication between a WX switch and groups of up to four RADIUS servers for remote authentication, authorization, and accounting (AAA) of administrators and network users.

<table>
<thead>
<tr>
<th>Commands by Usage</th>
<th>This chapter presents RADIUS commands alphabetically. Use Table 92 to locate commands in this chapter based on their uses.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Table 92</strong></td>
<td><strong>RADIUS Commands by Usage</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td><strong>Command</strong></td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>set radius client system-ip on page 632</td>
</tr>
<tr>
<td></td>
<td>clear radius client system-ip on page 627</td>
</tr>
<tr>
<td>RADIUS Servers</td>
<td>set radius on page 630</td>
</tr>
<tr>
<td></td>
<td>set radius server on page 635</td>
</tr>
<tr>
<td></td>
<td>clear radius on page 626</td>
</tr>
<tr>
<td></td>
<td>clear radius server on page 629</td>
</tr>
<tr>
<td>Server Groups</td>
<td>set server group on page 637</td>
</tr>
<tr>
<td></td>
<td>set server group load-balance on page 638</td>
</tr>
<tr>
<td></td>
<td>clear server group on page 629</td>
</tr>
<tr>
<td>RADIUS Proxy</td>
<td>set radius proxy client on page 633</td>
</tr>
<tr>
<td></td>
<td>set radius proxy port on page 634</td>
</tr>
<tr>
<td></td>
<td>clear radius proxy client on page 628</td>
</tr>
<tr>
<td></td>
<td>clear radius proxy port on page 628</td>
</tr>
</tbody>
</table>

(For information about RADIUS attributes, see the RADIUS appendix in the Wireless LAN Switch and Controller Configuration Guide.)
clear radius

Resets parameters that were globally configured for RADIUS servers to their default values.

**Syntax** — `clear radius {deadtime | key | retransmit | timeout }

deadtime — Number of minutes to wait after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server.

key — Password (shared secret key) used to authenticate to the RADIUS server.

retransmit — Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable.

timeout — Number of seconds to wait for the RADIUS server to respond before retransmitting.

**Defaults** — Global RADIUS parameters have the following default values:

- **deadtime**—0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)

- **key**—No key

- **retransmit**—3 (the total number of attempts, including the first attempt)

- **timeout**—5 seconds

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To override the globally set values on a particular RADIUS server, use the `set radius server` command.

**Examples** — To reset all global RADIUS parameters to their factory defaults, type the following commands:

```
WX4400# clear radius deadtime
success: change accepted.
WX4400# clear radius key
success: change accepted.
WX4400# clear radius retransmit
success: change accepted.
```
clear radius client system-ip

Removes the WX switch’s system IP address from use as the permanent source address in RADIUS client requests from the switch to its RADIUS server(s).

Syntax — clear radius client system-ip

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The clear radius client system-ip command causes the WX switch to use the IP address of the interface through which it sends a RADIUS client request as the source IP address. The WX switch selects a source interface address based on information in its routing table as the source address for RADIUS packets leaving the switch.

Examples — To clear the system IP address as the permanent source address for RADIUS client requests, type the following command:

```
WX4400# clear radius client system-ip
success: change accepted.
```

See Also

- display aaa on page 277
- set radius on page 630
- set radius server on page 635
<table>
<thead>
<tr>
<th>clear radius proxy client</th>
<th>Removes RADIUS proxy client entries for third-party APs.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong> — clear radius proxy client all</td>
<td></td>
</tr>
<tr>
<td><strong>Defaults</strong> — None.</td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong> — Enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>History</strong> — Introduced in MSS 4.0.</td>
<td></td>
</tr>
<tr>
<td><strong>Examples</strong> — The following command clears all RADIUS proxy client entries from the switch:</td>
<td></td>
</tr>
<tr>
<td>WX4400# clear radius proxy client all success: change accepted.</td>
<td></td>
</tr>
<tr>
<td><strong>See Also</strong></td>
<td></td>
</tr>
<tr>
<td>• set radius proxy client on page 633</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear radius proxy port</th>
<th>Removes RADIUS proxy ports configured for third-party APs.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Syntax</strong> — clear radius proxy port all</td>
<td></td>
</tr>
<tr>
<td><strong>Defaults</strong> — None.</td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong> — Enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>History</strong> — Introduced in MSS 4.0.</td>
<td></td>
</tr>
<tr>
<td><strong>Examples</strong> — The following command clears all RADIUS proxy port entries from the switch:</td>
<td></td>
</tr>
<tr>
<td>WX4400# clear radius proxy port all success: change accepted.</td>
<td></td>
</tr>
<tr>
<td><strong>See Also</strong></td>
<td></td>
</tr>
<tr>
<td>• set radius proxy port on page 634</td>
<td></td>
</tr>
</tbody>
</table>
clear radius server

Removes the named RADIUS server from the WX configuration.

**Syntax** — clear radius server **server-name**

- **server-name** — Name of a RADIUS server configured to perform remote AAA services for the WX switch.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following command removes the RADIUS server rs42 from a list of remote AAA servers:

```
WX4400# clear radius server rs42
success: change accepted.
```

**See Also**
- display aaa on page 277
- set radius server on page 635

---

clear server group

Removes a RADIUS server group from the configuration, or disables load balancing for the group.

**Syntax** — clear server group **group-name** [load-balance]

- **group-name** — Name of a RADIUS server group configured to perform remote AAA services for WX switches.
- **load-balance** — Ability of group members to share demand for services among servers.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — Deleting a server group removes the server group from the configuration. However, the members of the server group remain.
Examples — To remove the server group *sg-77* type the following command:

```
WX4400# clear server group sg-77
success: change accepted.
```

To disable load balancing in a server group *shorebirds*, type the following command:

```
WX4400# set server group shorebirds load-balance disable
success: change accepted.
```

See Also
- *set server group* on page 637

### set radius

Configures global defaults for RADIUS servers that do not explicitly set these values themselves. By default, the WX switch automatically sets all these values except the password (key).

**Syntax** — `set radius` `{deadtime minutes | encrypted-key string | key string | retransmit number | timeout seconds}`

- **deadtime minutes** — Number of minutes the WX switch waits after declaring an unresponsive RADIUS server unavailable before retrying the RADIUS server. You can specify from 0 to 1440 minutes.

- **encrypted keyword string** — Password (shared secret key) used to authenticate to the RADIUS server, entered in its encrypted form. You must provide the same encrypted password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.

MSS does not encrypt the string you enter, and instead displays the string in `display config` and `display aaa` output exactly as you entered it.

**Note**: Use this option only if you are entering the key in its encrypted form. To enter the key in unencrypted form, use the **key string** option instead.

- **key string** — Password (shared secret key) used to authenticate to the RADIUS server. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.
MSS encrypts the display form of the string in display config and display aaa output.

- **retransmit number** — Number of transmission attempts the WX switch makes before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.

- **timeout seconds** — Number of seconds the WX switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535.

**Defaults** — Global RADIUS parameters have the following default values:

- **deadtime** — 0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)

- **encrypted-key** — No key

- **key** — No key

- **retransmit** — 3 (the total number of attempts, including the first attempt)

- **timeout** — 5 seconds

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. The **encrypted-key** option was added in Version 4.2.

**Usage** — You can specify only one parameter per command line.

**Examples** — The following commands sets the dead time to 5 minutes, the RADIUS key to goody, the number of retransmissions to 1, and the timeout to 21 seconds on all RADIUS servers connected to the WX switch:

```
WX1200# set radius deadtime 5
success: change accepted.
WX1200# set radius key goody
success: change accepted.
WX1200# set radius retransmit 1
success: change accepted.
WX1200# set radius timeout 21
success: change accepted.
```
See Also

- `clear radius server` on page 629
- `display aaa` on page 277
- `set radius server` on page 635

**set radius client system-ip**

Causes all RADIUS requests to be sourced from the IP address specified by the `set system ip-address` command, providing a permanent source IP address for RADIUS packets sent from the WX switch.

**Syntax** — `set radius client system-ip`

**Defaults** — None. If you do not use this command, RADIUS packets leaving the WX have the source IP address of the outbound interface, which can change as routing conditions change.

**Examples** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — The WX system IP address must be set before you use this command.

**Examples** — The following command sets the WX system IP address as the address of the RADIUS client:

```
WX4400# set radius client system-ip
success: change accepted.
```

See Also

- `clear radius client system-ip` on page 627
- `set system idle-timeout` on page 113
**set radius proxy client**

Adds a RADIUS proxy entry for a third-party AP. The proxy entry specifies the IP address of the AP and the UDP ports on which the WX switch listens for RADIUS traffic from the AP.

**Syntax** — `set radius proxy client address ip-address [acct-port acct-udp-port-number] [port udp-port-number] key string`

- `address ip-address` — IP address of the third-party AP. Enter the address in dotted decimal notation.
- `port udp-port-number` — UDP port on which the WX switch listens for RADIUS access-requests from the AP.
- `acct-port acct-udp-port-number` — UDP port on which the WX switch listens for RADIUS stop-accounting records from the AP.
- `key string` — Password (shared secret key) the WX switch uses to authenticate and encrypt RADIUS communication.

**Defaults** — The default UDP port number for access-requests is 1812. The default UDP port number for stop-accounting records is 1813.

**Access** — Enabled.

**History** — Introduced in MSS 4.0.

**Usage** — AAA for third-party AP users has additional configuration requirements. See the “Configuring AAA for Users of Third-Party APs” section in the “Configuring AAA for Network Users” chapter of the Wireless LAN Switch and Controller Configuration Guide.

**Examples** — The following command configures a RADIUS proxy entry for a third-party AP RADIUS client at 10.20.20.9, sending RADIUS traffic to the default UDP ports 1812 and 1813 on the WX:

```
WX4400# set radius proxy client address 10.20.20.9 key radkey1
success: change accepted.
```

**See Also**

- `clear radius proxy client` on page 628
- `set authentication proxy` on page 301
- `set radius proxy port` on page 634
**set radius proxy port**

Configures the WX port connected to a third-party AP as a RADIUS proxy for the SSID supported by the AP.

**Syntax** — `set radius proxy port port-list [tag tag-value] ssid ssid-name`

- `port port-list` — WX port(s) connected to the third-party AP.
- `tag tag-value` — 802.1Q tag value in packets sent by the third-party AP for the SSID.
- `ssid ssid-name` — SSID supported by the third-party AP.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS 4.0.

**Usage** — AAA for third-party AP users has additional configuration requirements. See the “Configuring AAA for Users of Third-Party APs” section in the “Configuring AAA for Network Users” chapter of the Wireless LAN Switch and Controller Configuration Guide.

Enter a separate command for each SSID, and its tag value, you want the WX to support.

**Examples** — The following command maps SSID `mycorp` to packets received on port 3 or 4, using 802.1Q tag value 104:

```
WX4400# set radius proxy port 3-4 tag 104 ssid mycorp
success: change accepted.
```

**See Also**

- `clear radius proxy port` on page 628
- `set authentication proxy` on page 301
- `set radius proxy client` on page 633
set radius server

Configures RADIUS servers and their parameters. By default, the WX switch automatically sets all these values except the password (key).

**Syntax** — set radius server server-name
[address ip-address] [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit number] [deadtime minutes] [key string] encrypted-key string] [author-password password]

- server-name — Unique name for this RADIUS server. Enter an alphanumeric string of up to 32 characters, with no blanks.
- address ip-address — IP address of the RADIUS server. Enter the address in dotted decimal notation.
- auth-port port-number — UDP port that the WX switch uses for authentication and authorization.
- acct-port port-number — UDP port that the WX switch uses for accounting.
- timeout seconds — Number of seconds the WX switch waits for the RADIUS server to respond before retransmitting. You can specify from 1 to 65,535 seconds.
- retransmit number — Number of transmission attempts made before declaring an unresponsive RADIUS server unavailable. You can specify from 1 to 100 retries.
- deadtime minutes — Number of minutes the WX switch waits after declaring an unresponsive RADIUS server unavailable before retrying that RADIUS server. Specify between 0 (zero) and 1440 minutes (24 hours). A zero value causes the switch to identify unresponsive servers as available.
- key string — Password (shared secret key) the WX switch uses to authenticate to the RADIUS server. You must provide the same password that is defined on the RADIUS server. The password can be 1 to 64 characters long, with no spaces or tabs.
  - Use the **key** option to enter the string in its unencrypted form. MSS encrypts the displayed form of the string in **display config** and **display aaa** output.
  - To enter the string in its encrypted form instead, use the **encrypted-key** option. MSS does not encrypt the string you enter, and instead displays the string exactly as you enter it.
- **author-password** *password* — Password used for authorization to a RADIUS server for MAC users. Specify a password of up to 64 alphanumeric characters with no spaces or tabs.

**Defaults** — Default values are listed below:

- **auth-port** — UDP port 1812
- **acct-port** — UDP port 1813
- **timeout** — 5 seconds
- **retransmit** — 3 (the total number of attempts, including the first attempt)
- **deadtime** — 0 (zero) minutes (The WX switch does not designate unresponsive RADIUS servers as unavailable.)
- **key** — No key
- **encrypted-key** — No key
- **author-password** — When using RADIUS for authentication, a MAC user’s MAC address is also used as the default authorization password for that user, and no global authorization password is set. A last-resort user’s default authorization password is *3Com*.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. The **encrypted-key** option was added in Version 4.2.

**Usage** — For a given RADIUS server, the first instance of this command must set both the server name and the IP address and can include any or all of the other optional parameters. Subsequent instances of this command can be used to set optional parameters for a given RADIUS server.

To configure the server as a remote authenticator for the WX switch, you must add it to a server group with the **set server group** command.

Do not use the same name for a RADIUS server and a RADIUS server group.
Examples — To set a RADIUS server named RS42 with IP address 198.162.1.1 to use the default accounting and authorization ports with a timeout interval of 30 seconds, two transmit attempts, 5 minutes of dead time, and a key string of keys4u, type the following command:

```
WX1200# set radius server RS42 address 198.162.1.1 timeout 30 retransmit 2 deadtime 5 key keys4u
```

See Also
- display aaa on page 277
- set authentication admin on page 287
- set authentication console on page 289
- set authentication dot1x on page 291
- set authentication mac on page 295
- set authentication mac on page 295
- set authentication web on page 302
- set radius on page 630
- set server group on page 637

---

**set server group**

Configures a group of one to four RADIUS servers.

**Syntax**

```bash
set server group group-name members server-name1 [server-name2] [server-name3] [server-name4]
```

- **group-name** — Server group name of up to 32 characters, with no spaces or tabs.
- **members server-name1, server-name2, server-name3, server-name4** — The names of one or more configured RADIUS servers. You can enter up to four server names.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You must assign all group members simultaneously, as shown in the example. To enable load balancing, use **set server group load-balance enable**.
Do not use the same name for a RADIUS server and a RADIUS server group.

**Examples** — To set server group *shorebirds* with members *heron*, *egret*, and *sandpiper*, type the following command:

```
WX1200# set server group shorebirds members heron egret sandpiper
success: change accepted.
```

**See Also**

- `clear server group` on page 629
- `display aaa` on page 277
- `set server group load-balance` on page 638

---

**set server group load-balance**

Enables or disables load balancing among the RADIUS servers in a server group.

**Syntax** — `set server group group-name load-balance {enable | disable}`

- `group-name` — Server group name of up to 32 characters.
- `load-balance enable | disable` — Enables or disables load balancing of authentication requests among the servers in the group.

**Defaults** — Load balancing is disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You can optionally enable load balancing after assigning the server group members. If you configure load balancing, MSS sends each AAA request to a separate server, starting with the first one on the list and skipping unresponsive servers. If no server in the group responds, MSS moves to the next method configured with `set authentication` and `set accounting`.

In contrast, if load balancing is not configured, MSS always begins with the first server in the list and sends unfulfilled requests to each subsequent server in the group before moving on to the next configured AAA method.
Examples — To enable load balancing between the members of server group `shorebirds`, type the following command:

```
WX1200# set server group shorebirds load-balance enable
success: change accepted.
```

To disable load balancing between `shorebirds` server group members, type the following command:

```
WX1200# set server group shorebirds load-balance disable
success: change accepted.
```

See Also
- `clear server group` on page 629
- `clear radius server` on page 629
- `display aaa` on page 277
- `set server group` on page 637
17 802.1X MANAGEMENT COMMANDS

Use 802.1X management commands to modify the default settings for IEEE 802.1X sessions on an WX. For best results, change the settings only if you are aware of a problem with 802.1X performance on the WX.

**CAUTION:** 802.1X parameter settings are global for all SSIDs configured on the switch.

### Commands by Usage

This chapter presents 802.1X commands alphabetically. Use Table 93 to locate commands in this chapter based on their use. For information about configuring 802.1X commands for user authentication, see “AAA Commands” on page 259.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired Authentication Port Control</td>
<td><em>set dot1x port-control</em> on page 654</td>
</tr>
<tr>
<td></td>
<td><em>clear dot1x port-control</em> on page 643</td>
</tr>
<tr>
<td></td>
<td><em>set dot1x authcontrol</em> on page 650</td>
</tr>
<tr>
<td>Keys</td>
<td><em>set dot1x key-tx</em> on page 652</td>
</tr>
<tr>
<td></td>
<td><em>set dot1x tx-period</em> on page 658</td>
</tr>
<tr>
<td></td>
<td><em>clear dot1x tx-period</em> on page 647</td>
</tr>
<tr>
<td></td>
<td><em>set dot1x wep-rekey</em> on page 659</td>
</tr>
<tr>
<td></td>
<td><em>set dot1x wep-rekey-period</em> on page 660</td>
</tr>
<tr>
<td>Bonded Authentication</td>
<td><em>clear dot1x bonded-period</em> on page 642</td>
</tr>
<tr>
<td></td>
<td><em>set dot1x bonded-period</em> on page 651</td>
</tr>
<tr>
<td>Reauthentication</td>
<td><em>set dot1x reauth</em> on page 655</td>
</tr>
<tr>
<td></td>
<td><em>set dot1x reauth-max</em> on page 656</td>
</tr>
<tr>
<td>Reauthentication, cont.</td>
<td><em>clear dot1x reauth-max</em> on page 645</td>
</tr>
</tbody>
</table>
CHAPTER 17: 802.1X MANAGEMENT COMMANDS

Table 93  802.1X Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retransmission</td>
<td>set dot1x reauth-period</td>
</tr>
<tr>
<td></td>
<td>clear dot1x reauth-period</td>
</tr>
<tr>
<td>Quiet Period and Timeouts</td>
<td>set dot1x quiet-period</td>
</tr>
<tr>
<td></td>
<td>clear dot1x quiet-period</td>
</tr>
<tr>
<td></td>
<td>set dot1x timeout auth-server</td>
</tr>
<tr>
<td></td>
<td>clear dot1x timeout auth-server</td>
</tr>
<tr>
<td></td>
<td>set dot1x timeout supplicant</td>
</tr>
<tr>
<td></td>
<td>clear dot1x timeout supplicant</td>
</tr>
<tr>
<td>Settings, Active Clients, and Statistics</td>
<td>display dot1x</td>
</tr>
</tbody>
</table>

**clear dot1x bonded-period**

Resets the Bonded Auth™ (bonded authentication) period to its default value. The bonded period is the number of seconds MSS retains session information for an authenticated machine while waiting for an 802.1X client on the machine to start (re)authentication for the user. When bonded authentication is enabled, it applies only to an 802.1X user whose authentication rule on the WX switch contains the `bonded` option.

**Syntax** — clear dot1x bonded-period

**Defaults** — The default bonded authentication period is 0 seconds, which disables the feature.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To reset the Bonded period to its default, type the following command:

```
WX4400# clear dot1x bonded-period
success: change accepted.
```
clear dot1x max-req

Resets to the default setting the number of Extensible Authentication Protocol (EAP) requests that the WX switch retransmits to a supplicant (client).

Syntax — clear dot1x max-req

Defaults — The default number is 20.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To reset the number of 802.1X requests the WX can send to the default setting, type the following command:

```
WX4400# clear dot1x max-req
success: change accepted.
```

See Also

- display dot1x on page 647
- set dot1x bonded-period on page 651

---

clear dot1x port-control

Resets all wired authentication ports on the WX switch to default 802.1X authentication.

Syntax — clear dot1x port-control

By default, all wired authentication ports are set to auto and they process authentication requests as determined by the set authentication dot1x command.

Access — Enabled.

History — Introduced in MSS Version 3.0.
**clear dot1x quiet-period**

Resets the quiet period after a failed authentication to the default setting.

**Syntax** — clear dot1x quiet-period

**Defaults** — The default is 60 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to reset the 802.1X quiet period to the default:

```
WX4400# clear dot1x quiet-period
success: change accepted.
```

**See Also**

- display dot1x on page 647
- set dot1x quiet-period on page 655
**clear dot1x reauth-max**

Resets the maximum number of reauthorization attempts to the default setting.

**Syntax** — clear dot1x reauth-max

**Defaults** — The default is 2 attempts.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to reset the maximum number of reauthorization attempts to the default:

```
WX4400# clear dot1x reauth-max
success: change accepted.
```

**See Also**
- [display dot1x](#)
- [set dot1x reauth-max](#)

---

**clear dot1x reauth-period**

Resets the time period that must elapse before a reauthentication attempt, to the default time period.

**Syntax** — clear dot1x reauth-period

**Defaults** — The default is 3600 seconds (1 hour).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to reset the default reauthentication time period:

```
WX4400# clear dot1x reauth-period
success: change accepted.
```

**See Also**
- [display dot1x](#)
- [set dot1x reauth-period](#)
**clear dot1x timeout auth-server**

Resets to the default setting the number of seconds that must elapse before the WX times out a request to a RADIUS server.

**Syntax** — `clear dot1x timeout auth-server`

**Defaults** — The default is 30 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To reset the default timeout for requests to an authentication server, type the following command:

```
WX4400# clear dot1x timeout auth-server
success: change accepted.
```

**See Also**

- "display dot1x on page 647"
- "set dot1x timeout auth-server on page 657"

---

**clear dot1x timeout supplicant**

Resets to the default setting the number of seconds that must elapse before the WX switch times out an authentication session with a supplicant (client).

**Syntax** — `clear dot1x timeout supplicant`

**Defaults** — The default for the authentication timeout sessions is 30 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to reset the timeout period for an authentication session:

```
WX4400# clear dot1x timeout supplicant
success: change accepted.
```

**See Also**

- "display dot1x on page 647"
- "set dot1x timeout supplicant on page 658"
clear dot1x tx-period

Resets to the default setting the number of seconds that must elapse before the WX switch retransmits an EAP over LAN (EAPoL) packet.

**Syntax** — clear dot1x tx-period

**Defaults** — The default is 5 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to reset the EAPoL retransmission time:

WX4400# clear dot1x tx-period

success: change accepted.

**See Also**
- display dot1x on page 647
- set dot1x tx-period on page 658

---

display dot1x

Displays 802.1X client information for statistics and configuration settings.

**Syntax** — display dot1x {clients | stats | config}

- **clients** — Displays information about active 802.1X clients, including client name, MAC address, and state.
- **stats** — Displays global 802.1X statistics associated with connecting and authenticating.
- **config** — Displays a summary of the current configuration.

**Defaults** — None.

**Access** — Enabled.
History — Introduced in MSS Version 3.0. Format of 802.1X authentication rule information in display dot1x config output changed in MSS Version 3.2. The rules are still listed at the top of the display, but more information is shown for each rule.

Examples — Type the following command to display the 802.1X clients:

```
WX4400# display dot1x clients
MAC Address               State        Vlan             Identity
-------------             -------      ------           ----------
00:20:a6:48:01:1f       Connecting      (unknown)       
00:05:3c:07:6d:7c       Authenticated   vlan-it         EXAMPLE\jose
00:05:5d:7e:94:83       Authenticated   vlan-eng        EXAMPLE\singh
00:02:2d:86:bd:38       Authenticated   vlan-eng        bard@xmple.com
00:05:5d:7e:97:b4       Authenticated   vlan-eng        EXAMPLE\havel
00:05:5d:7e:98:1a       Authenticated   vlan-eng        EXAMPLE\nash
00:0b:be:a9:dc:4e       Authenticated   vlan-pm         xalik@xmple.com
00:05:5d:7e:96:e3       Authenticated   vlan-eng        EXAMPLE\mishan
00:02:2d:6f:44:77       Authenticated   vlan-eng        EXAMPLE\ethan
00:05:5d:7e:94:89       Authenticated   vlan-eng        EXAMPLE\fmarshall
00:06:80:00:5c:02       Authenticated   vlan-eng        EXAMPLE\bmccarthy
00:02:2d:6a:de:f2       Authenticated   vlan-pm         neailey@xmple.com
00:02:2d:5e:5b:76       Authenticated   vlan-pm         EXAMPLE\tamara
00:02:2d:80:b6:e1       Authenticated   vlan-cs         dmc@xmple.com
00:30:65:16:8d:69       Authenticated   vlan-wep        MAC authenticated
00:02:2d:64:8e:1b       Authenticated   vlan-eng        EXAMPLE\wong
```

Type the following command to display the 802.1X configuration:

```
WX1200# display dot1x config
802.1X user policy
---------------------
'host/bob-laptop.mycorp.com' on ssid 'mycorp' doing PASSTHRU
'bob.mycorp.com' on ssid 'mycorp' doing PASSTHRU (bonded)
```
<table>
<thead>
<tr>
<th>802.1X parameter</th>
<th>setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>supplicant timeout</td>
<td>30</td>
</tr>
<tr>
<td>auth-server timeout</td>
<td>30</td>
</tr>
<tr>
<td>quiet period</td>
<td>5</td>
</tr>
<tr>
<td>transmit period</td>
<td>5</td>
</tr>
<tr>
<td>reauthentication period</td>
<td>3600</td>
</tr>
<tr>
<td>maximum requests</td>
<td>2</td>
</tr>
<tr>
<td>key transmission</td>
<td>enabled</td>
</tr>
<tr>
<td>reauthentication</td>
<td>enabled</td>
</tr>
<tr>
<td>authentication control</td>
<td>enabled</td>
</tr>
<tr>
<td>WEP rekey period</td>
<td>1800</td>
</tr>
<tr>
<td>WEP rekey</td>
<td>enabled</td>
</tr>
<tr>
<td>Bonded period</td>
<td>60</td>
</tr>
</tbody>
</table>

- port 5, authcontrol: auto, max-sessions: 16
- port 6, authcontrol: auto, max-sessions: 1
- port 7, authcontrol: auto, max-sessions: 1
- port 8, authcontrol: auto, max-sessions: 1

Type the following command to display 802.1X statistics:

```
WX4400# display dot1x stats
```

<table>
<thead>
<tr>
<th>802.1X statistic</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enters Connecting:</td>
<td>709</td>
</tr>
<tr>
<td>Logoffs While Connecting:</td>
<td>112</td>
</tr>
<tr>
<td>Enters Authenticating:</td>
<td>467</td>
</tr>
<tr>
<td>Success While Authenticating:</td>
<td>0</td>
</tr>
<tr>
<td>Timeouts While Authenticating:</td>
<td>52</td>
</tr>
<tr>
<td>Failures While Authenticating:</td>
<td>0</td>
</tr>
<tr>
<td>Reauths While Authenticating:</td>
<td>0</td>
</tr>
<tr>
<td>Starts While Authenticating:</td>
<td>31</td>
</tr>
<tr>
<td>Logoffs While Authenticating:</td>
<td>0</td>
</tr>
<tr>
<td>Starts WhileAuthenticated:</td>
<td>85</td>
</tr>
<tr>
<td>Logoffs WhileAuthenticated:</td>
<td>1</td>
</tr>
<tr>
<td>Bad Packets Received:</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 94 explains the counters in the display dot1x stats output.
CHAPTER 17: 802.1X MANAGEMENT COMMANDS

set dot1x authcontrol

Provides a global override mechanism for 802.1X authentication configuration on wired authentication ports.

Syntax — set dot1x authcontrol {enable | disable}

- **enable** — Allows all wired authentication ports running 802.1X to use the authentication specified per port by the set dot1x port-control command.

- **disable** — Forces all wired authentication ports running 802.1X to unconditionally accept all 802.1X authentication attempts with an EAP Success message (ForceAuth).

Table 94  display dot1x stats Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enters Connecting</td>
<td>Number of times that the WX switch state transitions to the CONNECTING state from any other state.</td>
</tr>
<tr>
<td>Logoffs While</td>
<td>Number of times that the WX switch state transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPoL-Logoff message.</td>
</tr>
<tr>
<td>Connecting</td>
<td></td>
</tr>
<tr>
<td>Enters Authenticating</td>
<td>Number of times that the state wildcard transitions.</td>
</tr>
<tr>
<td>Success While</td>
<td>Number of times the WX switch state wildcard transitions from AUTHENTICATING from AUTHENTICATED, as a result of an EAP-Response/Identity message being received from the supplicant (client).</td>
</tr>
<tr>
<td>Authenticating</td>
<td></td>
</tr>
<tr>
<td>Timeouts While</td>
<td>Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING.</td>
</tr>
<tr>
<td>Authenticating</td>
<td></td>
</tr>
<tr>
<td>Failures While</td>
<td>Number of times that the WX switch state wildcard transitions from AUTHENTICATION to HELD.</td>
</tr>
<tr>
<td>Authenticating</td>
<td></td>
</tr>
<tr>
<td>Reauths While</td>
<td>Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE).</td>
</tr>
<tr>
<td>Authenticating</td>
<td></td>
</tr>
<tr>
<td>Starts While</td>
<td>Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-Start message being received from the Supplicant (client).</td>
</tr>
<tr>
<td>Authenticating</td>
<td></td>
</tr>
<tr>
<td>Logoffs While</td>
<td>Number of times that the WX switch state wildcard transitions from AUTHENTICATING to ABORTING, as a result of an EAPoL-logoff message being received from the Supplicant (client).</td>
</tr>
<tr>
<td>Authenticating</td>
<td></td>
</tr>
<tr>
<td>Bad Packets Received</td>
<td>Number of EAPoL packets received that have an invalid version or type.</td>
</tr>
</tbody>
</table>
**set dot1x bonded-period**

Changes the Bonded Auth™ (bonded authentication) period, which is the number of seconds MSS retains session information for an authenticated machine while waiting for the 802.1X client on the machine to start (re)authentication for the user.

You must set the bonded period to longer than 0 seconds to enable bonded authentication.

**Syntax** — `set dot1x bonded-period seconds`

- **seconds** — Number of seconds MSS retains session information for an authenticated machine while waiting for a client to (re)authenticate on the same machine. You can change the bonded authentication period to a value from 1 to 300 seconds.

**Defaults** — The default bonded period is 0 seconds, which disables the feature.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
**Usage** — Normally, the Bonded Auth period needs to be set only if the network has Bonded Auth clients that use dynamic WEP, or use WEP-40 or WEP-104 encryption with WPA or RSN. These clients can be affected by the 802.1X reauthentication parameter or the RADIUS Session-Timeout parameter.

3Com recommends that you try 60 seconds, and change the period to a longer value only if clients are unable to authenticate within 60 seconds.

The bonded authentication period applies only to 802.1X authentication rules that contain the **bonded** option.

**Examples** — To set the bonded authentication period to 60 seconds, type the following command:

```
WX4400# set dot1x bonded-period 60
success: change accepted.
```

**See Also**

- [display dot1x](#) on page 647
- [clear dot1x bonded-period](#) on page 642

---

**set dot1x key-tx** Enables or disables the transmission of encryption key information to the supplicant (client) in EAP over LAN (EAPoL) key messages, after authentication is successful.

**Syntax** — `set dot1x key-tx {enable | disable}`

- **enable** — Enables transmission of encryption key information to clients.
- **disable** — Disables transmission of encryption key information to clients.

**Defaults** — Key transmission is enabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
set dot1x max-req

Examples — Type the following command to enable key transmission:

WX4400# set dot1x key-tx enable
success: dot1x key transmission enabled.

See Also

- display dot1x on page 647

set dot1x max-req

Sets the maximum number of times the WX retransmits an EAP request to a supplicant (client) before ending the authentication session.

Syntax — set dot1x max-req number-of-retransmissions

- number-of-retransmissions — Specify a value between 0 and 10.

Defaults — The default number of EAP retransmissions is 2.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — To support SSIDs that have both 802.1X and static WEP clients, MSS sends a maximum of two ID requests, even if this parameter is set to a higher value. Setting the parameter to a higher value does affect all other types of EAP messages.

Examples — Type the following command to set the maximum number of EAP request retransmissions to three attempts:

WX4400# set dot1x max-req 3
success: dot1x max request set to 3.

See Also

- clear dot1x max-req on page 643
- display dot1x on page 647
**set dot1x port-control**

Determines the 802.1X authentication behavior on individual wired authentication ports or groups of ports.

**Syntax** — set dot1x port-control 
{forceauth | forceunauth | auto} port-list

- **forceauth** — Forces the specified wired authentication port(s) to *unconditionally authorize* all 802.1X authentication attempts, with an EAP success message.
- **forceunauth** — Forces the specified wired authentication port(s) to *unconditionally reject* all 802.1X authentication attempts with an EAP failure message.
- **auto** — Allows the specified wired authentication ports to process 802.1X authentication normally as determined for the user by the set authentication dot1X command.
- **port-list** — One or more wired authentication ports for which to set 802.1X port control.

**Defaults** — By default, wired authentication ports are set to *auto*.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command affects only wired authentication ports.

**Examples** — The following command forces port 1 to unconditionally accept all 802.1X authentication attempts:

WX4400# set dot1x port-control forceauth 1
success: authcontrol for 1 is set to FORCE-AUTH.

**See Also**

- *display port status* on page 127
- *display dot1x* on page 647
**set dot1x quiet-period**

Sets the number of seconds a WX remains quiet and does not respond to a supplicant after a failed authentication.

**Syntax** — `set dot1x quiet-period seconds`

- `seconds` — Specify a value between 0 and 65,535.

**Defaults** — The default is 60 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to set the quiet period to 90 seconds:

```
WX4400# set dot1x quiet-period 90
success: dot1x quiet period set to 90.
```

**See Also**

- `clear dot1x quiet-period` on page 644
- `set dot1x wep-rekey-period` on page 660

---

**set dot1x reauth**

Determines whether the WX switch allows the reauthentication of supplicants (clients).

**Syntax** — `set dot1x reauth {enable | disable}`

- `enable` — Permits reauthentication.
- `disable` — Denies reauthentication.

**Defaults** — Reauthentication is enabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to enable reauthentication of supplicants (clients):

```
WX4400# set dot1x reauth enable
success: dot1x reauthentication enabled.
```
set dot1x reauth-max

Sets the number of reauthentication attempts that the WX switch makes before the supplicant (client) becomes unauthorized.

**Syntax** — `set dot1x reauth-max number-of-attempts`

- `number-of-attempts` — Specify a value between 1 and 10.

**Defaults** — The default number of reauthentication attempts is 2.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — If the number of reauthentications for a wired authentication client is greater than the maximum number of reauthentications allowed, MSS sends an EAP failure packet to the client and removes the client from the network. However, MSS does not remove a wireless client from the network under these circumstances.

**Examples** — Type the following command to set the number of authentication attempts to 8:

```
WX4400# set dot1x reauth-max 8
success: dot1x max reauth set to 8.
```

**See Also**

- `display dot1x` on page 647
- `set dot1x reauth-max` on page 656
- `set dot1x reauth-period` on page 657
### set dot1x reauth-period

Sets the number of seconds that must elapse before the WX switch attempts reauthentication.

**Syntax** — `set dot1x reauth-period seconds`

- **seconds** — Specify a value between 60 (1 minute) and 1,641,600 (19 days).

**Defaults** — The default is 3600 seconds (1 hour).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to set the number of seconds to 100 before reauthentication is attempted:

```
WX4400# set dot1x reauth-period 100
success: dot1x auth-server timeout set to 100.
```

**See Also**
- `display dot1x` on page 647
- `clear dot1x reauth-period` on page 645

### set dot1x timeout auth-server

Sets the number of seconds that must elapse before the WX switch times out a request to a RADIUS authentication server.

**Syntax** — `set dot1x timeout auth-server seconds`

- **seconds** — Specify a value between 1 and 65,535.

**Defaults** — The default is 30 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to set the authentication server timeout to 60 seconds:

```
WX4400# set dot1x timeout auth-server 60
success: dot1x auth-server timeout set to 60.
```
**set dot1x timeout supplicant**

Sets the number of seconds that must elapse before the WX switch times out an authentication session with a supplicant (client).

**Syntax** — `set dot1x timeout supplicant seconds`

- `seconds` — Specify a value between 1 and 65,535.

**Defaults** — The default is 30 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to set the number of seconds for authentication session timeout to 300:

```
WX4400# set dot1x timeout supplicant 300
success: dot1x supplicant timeout set to 300.
```

**See Also**

- `display dot1x` on page 647
- `clear dot1x timeout auth-server` on page 646

---

**set dot1x tx-period**

Sets the number of seconds that must elapse before the WX switch retransmits an EAPoL packet.

**Syntax** — `set dot1x tx-period seconds`

- `seconds` — Specify a value between 1 and 65,535.

**Defaults** — The default is 5 seconds.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
Examples — Type the following command to set the number of seconds before the WX switch retransmits an EAPoL packet to 300:

WX4400# set dot1x tx-period 300
success: dot1x tx-period set to 300.

See Also

- display dot1x on page 647
- clear dot1x tx-period on page 647
set dot1x wep-rekey-period

Sets the interval for rotating the WEP broadcast and multicast keys.

**Syntax** — `set dot1x wep-rekey-period seconds`

- **seconds** — Specify a value between 30 and 1,641,600 (19 days).

**Defaults** — The default is 1800 seconds (30 minutes).

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to set the WEP-rekey period to 300 seconds:

```
WX4400# set dot1x wep-rekey-period 300
success: dot1x wep-rekey-period set to 300
```

**See Also**

- `display dot1x` on page 647
- `set dot1x wep-rekey` on page 659
Use session management commands to display and clear administrative and network user sessions.

This chapter presents session management commands alphabetically. Use Table 95 to locate commands in this chapter based on their use.

### Table 95  Session Management Commands by Usage

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Sessions</td>
<td><code>display sessions</code> on page 664</td>
</tr>
<tr>
<td></td>
<td><code>clear sessions</code> on page 661</td>
</tr>
<tr>
<td>Network Sessions</td>
<td><code>display sessions network</code> on page 668</td>
</tr>
<tr>
<td></td>
<td><code>clear sessions network</code> on page 663</td>
</tr>
<tr>
<td>Mesh AP Sessions</td>
<td><code>display sessions mesh-ap</code> on page 667</td>
</tr>
</tbody>
</table>

### clear sessions

Clears all administrative sessions, or clears administrative console or Telnet sessions.

**Syntax** — clear sessions {admin | console | telnet [client [session-id] | mesh-ap [session-id] session-id]}

- **admin** — Clears sessions for all users with administrative access to the WX switch through a Telnet or SSH connection or a console plugged into the switch.
- **console** — Clears sessions for all users with administrative access to the WX switch through a console plugged into the switch.
- **telnet** — Clears sessions for all users with administrative access to the WX switch through a Telnet connection.
• **telnet client** \([session-id]\) — Clears all Telnet client sessions from the CLI to remote devices, or clears an individual session identified by session ID.

• **mesh-ap** \([session-id]\) — Clears all Mesh AP sessions, or clears an individual Mesh AP session identified by session ID.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To clear all administrator sessions type the following command:

```console
WX4400# clear sessions admin
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear all administrative sessions through the console, type the following command:

```console
WX4400# clear sessions console
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear all administrative Telnet sessions, type the following command:

```console
WX4400# clear sessions telnet
This will terminate manager sessions, do you wish to continue? (y|n) [n]y
```

To clear Telnet client session 0, type the following command:

```console
WX4400# clear sessions telnet client 0
```

**See Also**

• **display sessions** on page 664
**clear sessions network**

Clears all network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, virtual LAN (VLAN) or set of VLANs, or session ID.

**Syntax** — clear sessions network {user user-glob | mac-addr mac-addr-glob | vlan vlan-glob | session-id local-session-id}

- **user user-glob** — Clears all network sessions for a single user or set of users.
  
  Specify a username, use the double-asterisk wildcard character (***) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

- **mac-addr mac-addr-glob** — Clears all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:), or use the wildcard character (*) to specify a set of MAC addresses. (For details, see “MAC Address Globs” on page 79.)

- **vlan vlan-glob** — Clears all network sessions on a single VLAN or a set of VLANs.
  
  Specify a VLAN name, use the double-asterisk wildcard character (***) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “VLAN Globs” on page 80.)

- **session-id local-session-id** — Clears the specified 802.1X network session. To find local session IDs, use the display sessions command.

**Defaults** — None.

**Access** — Enabled.

**History** —Introduced in MSS Version 3.0.

**Usage** — The clear sessions network command clears network sessions by deauthenticating and, for wireless clients, disassociating them.
Examples — To clear all sessions for MAC address 00:01:02:03:04:05, type the following command:

WX4400# clear sessions network mac-addr 00:01:02:03:04:05

To clear session 9, type the following command:

WX1200# clear sessions network session-id 9

SM Apr 11 19:53:38 DEBUG SM-STATE: localid 9, mac 00:06:25:09:39:5d, flags 0000012fh, to change state to KILLING
Localid 9, globalid SESSION-9-893249336 moved from ACTIVE to KILLING
(client=00:06:25:09:39:5d)

To clear the session of user Natasha, type the following command:

WX1200# clear sessions network user Natasha

To clear the sessions of users whose name begins with the characters Jo, type the following command:

WX1200# clear sessions network user Jo*

To clear the sessions of all users on VLAN red, type the following command:

WX1200# clear sessions network vlan red

See Also

- display sessions on page 664
- display sessions network on page 668

display sessions

Displays session information and statistics for all users with administrative access to the WX switch, or for administrative users with either console or Telnet access.

Syntax —

```
display sessions {admin | console | telnet [client]}
```

- admin — Displays sessions for all users with administrative access to the WX switch through a Telnet or SSH connection or a console plugged into the switch.
- console — Displays sessions for all users with administrative access to the WX switch through a console plugged into the switch.
- **telnet** — Displays sessions for all users with administrative access to the WX switch through a Telnet connection.

- **telnet client** — Displays Telnet sessions from the CLI to remote devices.

**Defaults** — None.

**Access** — All, except for **display sessions telnet client**, which has enabled access.

**History** — Introduced in MSS Version 3.0.

**Examples** — To view information about sessions of administrative users, type the following command:

```
WX4400> display sessions admin
```

```
<table>
<thead>
<tr>
<th>Tty</th>
<th>Username</th>
<th>Time (s)</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>tty0</td>
<td></td>
<td>3644</td>
<td>Console</td>
</tr>
<tr>
<td>tty2</td>
<td>tech</td>
<td>6</td>
<td>Telnet</td>
</tr>
<tr>
<td>tty3</td>
<td>sshadmin</td>
<td>381</td>
<td>SSH</td>
</tr>
</tbody>
</table>
```

3 admin sessions

To view information about console users’ sessions, type the following command:

```
WX4400> display sessions console
```

```
<table>
<thead>
<tr>
<th>Tty</th>
<th>Username</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>console</td>
<td></td>
<td>8573</td>
</tr>
</tbody>
</table>
```

1 console session

To view information about Telnet users sessions, type the following command:

```
WX4400> display sessions telnet
```

```
<table>
<thead>
<tr>
<th>Tty</th>
<th>Username</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tty2</td>
<td>sea</td>
<td>7395</td>
</tr>
</tbody>
</table>
```
To view information about Telnet client sessions, type the following command:

```
WX4400# display sessions telnet client
```

<table>
<thead>
<tr>
<th>Session</th>
<th>Server Address</th>
<th>Server Port</th>
<th>Client Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>192.168.1.81</td>
<td>23</td>
<td>48000</td>
</tr>
<tr>
<td>1</td>
<td>10.10.1.22</td>
<td>23</td>
<td>48001</td>
</tr>
</tbody>
</table>

Table 96 describes the fields of the `display sessions admin`, `display sessions console`, and `display sessions telnet` displays.

### Table 96  display sessions admin, display sessions console, and display sessions telnet Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tty</td>
<td>The Telnet terminal number, or console for administrative users connected through the console port.</td>
</tr>
<tr>
<td>Username</td>
<td>Up to 30 characters of the name of an authenticated user.</td>
</tr>
<tr>
<td>Time (s)</td>
<td>Number of seconds the session has been active.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of administrative session:</td>
</tr>
<tr>
<td></td>
<td>- Console</td>
</tr>
<tr>
<td></td>
<td>- SSH</td>
</tr>
<tr>
<td></td>
<td>- Telnet</td>
</tr>
</tbody>
</table>

Table 97 describes the fields of the `display sessions telnet client` display.

### Table 97  display sessions telnet client Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session</td>
<td>Session number assigned by MSS when the client session is established.</td>
</tr>
<tr>
<td>Server Address</td>
<td>IP address of the remote device.</td>
</tr>
<tr>
<td>Server Port</td>
<td>TCP port number of the remote device’s TCP server.</td>
</tr>
<tr>
<td>Client Port</td>
<td>TCP port number MSS is using for the client side of the session.</td>
</tr>
</tbody>
</table>

See Also
- clear sessions on page 661
**display sessions mesh-ap**

Displays summary or verbose information about Mesh AP sessions on the WX.

**Syntax** — `display sessions mesh-ap [session-id session-id | verbose]`

- **session-id local-session-id** — Displays the specified Mesh AP session. To determine the local session ID for a Mesh AP session, use the `display sessions mesh-ap` command without the `session-id` option.

- **verbose** — Provides detailed output for all Mesh AP sessions.

**Defaults** — None.

**Access** — All.

**History** — Introduced in MSS Version 6.0.

**Examples** — To view information about Mesh AP sessions, type the following command:

```
WX> display sessions mesh-ap
```

<table>
<thead>
<tr>
<th>User Name</th>
<th>Sess ID</th>
<th>VLAN Name</th>
<th>Port/Radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0b:0e:17:bb:3f</td>
<td>2* 1.1.1.3</td>
<td>(none)</td>
<td>L AP 2/2</td>
</tr>
</tbody>
</table>

Table 98 describes the fields of `display sessions mesh-ap` output.

**Table 98 display sessions mesh-ap Output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The MAC address of the authenticated Mesh AP.</td>
</tr>
<tr>
<td>Sess ID</td>
<td>Locally unique number that identifies this session. An asterisk (*) next to a session ID indicates that the session is fully active.</td>
</tr>
<tr>
<td>IP or MAC Address</td>
<td>IP address of the Mesh AP.</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN associated with the session.</td>
</tr>
<tr>
<td>Port/Radio</td>
<td>Number of the port and radio through which the Mesh AP is accessing this session.</td>
</tr>
</tbody>
</table>
display sessions network

Displays summary or verbose information about all network sessions, or network sessions for a specified username or set of usernames, MAC address or set of MAC addresses, VLAN or set of VLANs, or session ID.

Syntax — display sessions network

user user-glob | mac-addr mac-addr-glob | ssid ssid-name
vlan vlan-glob | session-id session-id | wired] [verbose]

- **user user-glob** — Displays all network sessions for a single user or set of users.
  Specify a username, use the double-asterisk wildcard character (***) to specify all usernames, or use the single-asterisk wildcard character (*) to specify a set of usernames up to or following the first delimiter character—either an at sign (@) or a period (.). (For details, see “User Globs” on page 78.)

- **mac-addr mac-addr-glob** — Displays all network sessions for a MAC address. Specify a MAC address in hexadecimal numbers separated by colons (:).
  Or use the wildcard character (*) to specify a set of MAC addresses.
  (For details, see “MAC Address Globs” on page 79.)

- **ssid ssid-name** — Displays all network sessions for an SSID.

- **vlan vlan-glob** — Displays all network sessions on a single VLAN or a set of VLANs.
  Specify a VLAN name, use the double-asterisk wildcard character (***) to specify all VLAN names, or use the single-asterisk wildcard character (*) to specify a set of VLAN names up to or following the first delimiter character, either an at sign (@) or a period (.). (For details, see “VLAN Globs” on page 80.)

- **session-id session-id** — Displays the specified network session. To find local session IDs, use the display sessions command. The verbose option is not available with this form of the display sessions network command.

- **wired** — Displays all network sessions on wired authentication ports.

- **verbose** — Provides detailed output for all network sessions or ones displayed by username, MAC address, or VLAN name.
display sessions network

Defaults — None.

Access — All.

History — Introduced in MSS Version 3.0. Output added to the display network sessions verbose command to indicate the user’s authorization attributes and whether they were supplied through AAA or through configured SSID defaults in a service profile in MSS Version 4.1.

Usage — MSS displays information about network sessions in three types of displays. See the following tables for field descriptions.

- **Summary display** — See Table 99 on page 671.
- **Verbose display** — See Table 100 on page 672.
- **display sessions network session-id** display — See Table 101 on page 674.

Examples — To display summary information for all network sessions, type display sessions network. For example:

```
WX1200# display sessions network
User                                      Sess  IP or MAC         VLAN  Port/
Name                                      ID  Address           Name    Radio
------------------------------ ----  -----------------  -------- ----- ---------
EXAMPLE\Natasha                           4*  10.10.40.17        vlan-eng  3/1
host/laptop11.exmpl.com                   6*  10.10.40.16        vlan-eng  3/2
nin@exmpl.com                             539* 10.10.40.17   vlan-eng  1/1
EXAMPLE\hosni                              302* 10.10.40.10  vlan-eng  3/1
                                             563 00:0b:be:15:46:56 (none) 1/2
jose@exmpl.com                            380* 10.30.40.8  vlan-eng  1/1
00:30:65:16:8d:69                         443* 10.10.40.19  vlan-wep  3/1
EXAMPLE\Geetha                            459* 10.10.40.18  vlan-eng  3/2
8 sessions total
```

The following command displays summary information about the sessions for MAC address 00:05:5d:7e:98:1a:

```
WX1200# display sessions network mac-addr 00:05:5d:7e:98:1a
User                                      Sess  IP or MAC         VLAN  Port/
Name                                      ID  Address           Name    Radio
------------------------------ ----  -----------------  -------- ----- ---------
EXAMPLE\Havel                            13*  10.10.10.40  vlan-eng  1/2
```
CHAPTER 18: SESSION MANAGEMENT COMMANDS

The following command displays summary information about all the sessions of users whose names begin with E:

WX1200# display sessions network user E*
User Name          Sess  IP or MAC      VLAN   Port/
              ID  Address  Name ID Address       Name Radio
----------------- ----  ----------------- ------------ ----- 
EXAMPLE\Singh    12* 10.10.10.30  vlan-eng  3/2
EXAMPLE\Havel    13* 10.10.10.40  vlan-eng  1/2
2 sessions match criteria (of 3 total)

(Table 99 on page 671 describes the summary displays of display sessions network commands.)

The following command displays detailed (verbose) session information about user nin@example.com:

WX1200# display sessions network user nin@example.com verbose
User Name          Sess  IP or MAC      VLAN   Port/
              ID  Address  Name ID Address       Name Radio
------------------------------ ----  ----------------- ------------ ----- 
nin@example.com   5* 10.20.30.40  vlan-eng         1/1
Client MAC: 00:02:2d:6e:ab:a5  GID: SESS-5-000430-686792-d8b3c564
State: ACTIVE (prev AUTHORIZED)
now on: WX 192.168.12.7, AP/radio 1/1, AP 00:0b:0e:ff:00:3a, as of 00:00:24 ago
1 sessions match criteria (of 10 total)

The following command displays verbose output about the sessions of all current network users:

WX1200# display sessions network verbose
User Name          Sess  IP or MAC      VLAN   Port/
              ID  Address  Name ID Address       Name Radio
------------------------------ ----  ----------------- ------------ ----- 
SHUTTLE2\exmpl    6* 10.3.8.55  default         3/1
Client MAC: 00:06:25:13:08:33  GID: SESS-4-000404-98441-c807c14b
State: ACTIVE (prev AUTHORIZED)
now on: WX 10.3.8.103, AP/radio 3/1, AP 00:0b:0e:ff:00:3a, as of 00:00:24 ago
  from: WX 10.3.8.103, AP/radio 6/1, AP 00:0b:0e:00:05:ff, as of 00:10:37 ago
  from: WX 10.3.8.103, AP/radio 3/1, AP 00:0b:0e:ff:00:3a, as of 00:01:53 ago
Vlan-Name=default (service-profile)
Service-Type=2 (service-profile)
End-Date=52/06/07-08:57 (AAA)
The following command displays information about network session 27:

```
WX1200# display sessions network session-id 27
Global Id: SESS-27-000430-835586-58dfe5a
State: ACTIVE
Port/Radio: 3/1
MAC Address: 00:00:2d:6f:44:77
User Name: EXAMPLE Natasha
IP Address: 10.10.40.17
Vlan Name: vlan-eng
Tag: 1
Session Timeout: 1800
Authentication Method: PEAP, using server 10.10.70.20
Session statistics as updated from AP:
  Unicast packets in: 653
  Unicast bytes in: 46211
  Unicast packets out: 450
  Unicast bytes out: 50478
  Multicast packets in: 317
  Multicast bytes in: 10144
  Number of packets with encryption errors: 0
  Number of bytes with encryption errors: 0
  Last packet data rate: 2
  Last packet signal strength: -67 dBm
  Last packet data S/N ratio: 55
```

Table 99 describes the output of this command. For descriptions of the fields of `display sessions network session-id` output, see Table 101 on page 674.

**Table 99** display sessions network (summary) Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Up to 30 characters of the name of the authenticated user of this session.</td>
</tr>
</tbody>
</table>
### Table 99  display sessions network (summary) Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sess ID</td>
<td>Locally unique number that identifies this session. An asterisk (*) next to</td>
</tr>
<tr>
<td>IP or MAC Address</td>
<td>IP address of the session user, or the user's MAC address if the user has</td>
</tr>
<tr>
<td>VLAN Name</td>
<td>Name of the VLAN associated with the session.</td>
</tr>
<tr>
<td>Port/Radio</td>
<td>Number of the port and radio through which the user is accessing this</td>
</tr>
</tbody>
</table>

### Table 100  Additional display sessions network verbose Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client MAC</td>
<td>MAC address of the session user.</td>
</tr>
<tr>
<td>GID</td>
<td>Global session ID, a unique session number within a Mobility Domain.</td>
</tr>
</tbody>
</table>
display sessions network

State

- **AUTH, ASSOC REQ** — Client is being associated by the 802.1X protocol.
- **AUTH AND ASSOC** — Client is being associated by the 802.1X protocol, and the user is being authenticated.
- **AUTHORIZING** — User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization.
- **AUTHORIZED** — User has been authorized by an AAA method.
- **ACTIVE** — User’s AAA attributes have been applied, and the user is active on the network.
- **DEASSOCIATED** — One of the following:
  - Wireless client has sent the WX switch a disassociate message.
  - User associated with one of the current WX switch’s MAP access points has appeared at another WX switch in the Mobility Domain.
- **ROAMING AWAY** — The WX switch has been sent a request to transfer the user, who is roaming, to another WX switch.
- **STATUS UPDATED** — WX switch is receiving a final update from a MAP access point about the user, who has roamed away.
- **WEB_AUTHING** — User is being authenticated by WebAAA.
- **WIRED_AUTH'ING** — User is being authenticated by the 802.1X protocol on a wired authentication port.
- **KILLING** — User’s session is being cleared, because of 802.1X authentication failure, entry of a clear command, or some other event.

now on

- IP address and port and radio numbers of the session’s current WX switch, the MAC address of the MAP access point, and the last update time.

from

- IP address and port and radio numbers of the session’s previous WX switch, the MAC address of the MAP access point, and the last update time. Up to six roaming events are tracked in this display.

Vlan-Name

Service-Type

Authorization attributes for the user and how they were assigned. The authorization attributes can be assigned either by a RADIUS server or the local database (indicated in the output by AAA), or by SSID default settings in the service profile the user used to gain access to the network (indicated in the output by service-profile).

Vlan-Name

Service-Type

Authorization attributes for the user and how they were assigned. The authorization attributes can be assigned either by a RADIUS server or the local database (indicated in the output by AAA), or by SSID default settings in the service profile the user used to gain access to the network (indicated in the output by service-profile).

Table 100 Additional display sessions network verbose Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Status of the session:</td>
</tr>
<tr>
<td></td>
<td>- <strong>AUTH, ASSOC REQ</strong> — Client is being associated by the 802.1X protocol.</td>
</tr>
<tr>
<td></td>
<td>- <strong>AUTH AND ASSOC</strong> — Client is being associated by the 802.1X protocol, and the user is being authenticated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>AUTHORIZING</strong> — User has been authenticated (for example, by the 802.1X protocol and an AAA method), and is entering AAA authorization.</td>
</tr>
<tr>
<td></td>
<td>- <strong>AUTHORIZED</strong> — User has been authorized by an AAA method.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ACTIVE</strong> — User’s AAA attributes have been applied, and the user is active on the network.</td>
</tr>
<tr>
<td></td>
<td>- <strong>DEASSOCIATED</strong> — One of the following:</td>
</tr>
<tr>
<td></td>
<td>- Wireless client has sent the WX switch a disassociate message.</td>
</tr>
<tr>
<td></td>
<td>- User associated with one of the current WX switch’s MAP access points has appeared at another WX switch in the Mobility Domain.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ROAMING AWAY</strong> — The WX switch has been sent a request to transfer the user, who is roaming, to another WX switch.</td>
</tr>
<tr>
<td></td>
<td>- <strong>STATUS UPDATED</strong> — WX switch is receiving a final update from a MAP access point about the user, who has roamed away.</td>
</tr>
<tr>
<td></td>
<td>- <strong>WEB_AUTHING</strong> — User is being authenticated by WebAAA.</td>
</tr>
<tr>
<td></td>
<td>- <strong>WIRED_AUTH’ING</strong> — User is being authenticated by the 802.1X protocol on a wired authentication port.</td>
</tr>
<tr>
<td></td>
<td>- <strong>KILLING</strong> — User’s session is being cleared, because of 802.1X authentication failure, entry of a clear command, or some other event.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>now on</td>
</tr>
<tr>
<td></td>
<td>- IP address and port and radio numbers of the session’s current WX switch, the MAC address of the MAP access point, and the last update time.</td>
</tr>
<tr>
<td></td>
<td>from</td>
</tr>
<tr>
<td></td>
<td>- IP address and port and radio numbers of the session’s previous WX switch, the MAC address of the MAP access point, and the last update time. Up to six roaming events are tracked in this display.</td>
</tr>
<tr>
<td></td>
<td>Vlan-Name</td>
</tr>
<tr>
<td></td>
<td>Authorization attributes for the user and how they were assigned. The authorization attributes can be assigned either by a RADIUS server or the local database (indicated in the output by AAA), or by SSID default settings in the service profile the user used to gain access to the network (indicated in the output by service-profile).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Global Id</td>
<td>A unique session identifier within the Mobility Domain.</td>
</tr>
<tr>
<td>State</td>
<td>Status of the session:</td>
</tr>
<tr>
<td></td>
<td>• <strong>AUTH, ASSOC REQ</strong> — Client is being associated by the 802.1X protocol.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AUTH AND ASSOC</strong> — Client is being associated by the 802.1X protocol, and the user is being authenticated.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AUTHORIZED</strong> — User has been authorized by an AAA method.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ACTIVE</strong> — User’s AAA attributes have been applied, and the user is active on the network.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DEASSOCIATED</strong> — One of the following:</td>
</tr>
<tr>
<td></td>
<td>• Wireless client has sent the WX switch a disassociate message.</td>
</tr>
<tr>
<td></td>
<td>• User associated with one of the current WX switch’s MAP access points has appeared at another WX switch in the Mobility Domain.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ROAMING AWAY</strong> — The WX switch has been sent a request to transfer the user, who is roaming, to another WX switch.</td>
</tr>
<tr>
<td></td>
<td>• <strong>STATUS UPDATED</strong> — WX switch is receiving a final update from an MAP access point about the user, who has roamed away.</td>
</tr>
</tbody>
</table>
| Port/Radio    | Number of the port and radio through which the user is accessing this session.
| MAC address   | MAC address of the session user.                                             |
| User Name     | Name of the authenticated user of this session.                              |
| IP Address    | IP address of the session user.                                              |
| Vlan Name     | Name of the VLAN associated with the session.                                |
| Tag           | System-wide supported VLAN tag type.                                        |
| Session Timeout | Assigned session timeout in seconds.                                       |
### Table 101  
**display sessions network session-id Output (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>Extensible Authentication Protocol (EAP) type used to authenticate the session user, and the IP address of the authentication server.</td>
</tr>
<tr>
<td>Session statistics as updated from AP</td>
<td>Time the session statistics were last updated from the MAP access point, in seconds since a fixed standard date and time.</td>
</tr>
<tr>
<td>Unicast packets in</td>
<td>Total number of unicast packets received from the user by the WX (64-bit counter).</td>
</tr>
<tr>
<td>Unicast bytes in</td>
<td>Total number of unicast bytes received from the user by the WX (64-bit counter).</td>
</tr>
<tr>
<td>Unicast packets out</td>
<td>Total number of unicast packets sent by the WX to the user (64-bit counter).</td>
</tr>
<tr>
<td>Unicast bytes out</td>
<td>Total number of unicast bytes sent by the WX to the user (64-bit counter).</td>
</tr>
<tr>
<td>Multicast packets in</td>
<td>Total number of multicast packets received from the user by the WX (64-bit counter).</td>
</tr>
<tr>
<td>Multicast bytes in</td>
<td>Total number of multicast bytes received from the user by the WX (64-bit counter).</td>
</tr>
<tr>
<td>Number of packets with encryption errors</td>
<td>Total number of decryption failures.</td>
</tr>
<tr>
<td>Number of bytes with encryption errors</td>
<td>Total number of bytes with decryption errors.</td>
</tr>
<tr>
<td>Last packet data rate</td>
<td>Data transmit rate, in megabits per second (Mbps), of the last packet received by the MAP access point.</td>
</tr>
<tr>
<td>Last packet signal strength</td>
<td>Signal strength, in decibels referred to 1 milliwatt (dBm), of the last packet received by the MAP access point.</td>
</tr>
<tr>
<td>Last packet data S/N ratio</td>
<td>Signal-to-noise ratio of the last packet received by the MAP access point.</td>
</tr>
</tbody>
</table>

**See Also**
- clear sessions network on page 663
MSS automatically performs RF detection scans on enabled and disabled radios to detect rogue access points. A rogue access point is a BSSID (MAC address associated with an SSID) that does not belong to a 3Com switch and is not a member of the ignore list configured on the seed switch of the Mobility Domain. The ignore list is a list of third-party (friendly) BSSIDs that are not rogues.

MSS can issue countermeasures against rogue devices to prevent clients from being able to use them.

You can configure RF detection parameters only on the seed switch of a Mobility Domain.

This chapter presents RF detection commands alphabetically. Use Table 102 to locate the commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue Information</td>
<td>display rfdetect clients</td>
</tr>
<tr>
<td></td>
<td>display rfdetect mobility-domain</td>
</tr>
<tr>
<td></td>
<td>display rfdetect data</td>
</tr>
<tr>
<td></td>
<td>display rfdetect visible</td>
</tr>
<tr>
<td></td>
<td>display rfdetect counters</td>
</tr>
<tr>
<td>Countermeasures</td>
<td>display rfdetect countermeasures</td>
</tr>
<tr>
<td>Permitted Vendor List</td>
<td>set rfdetect vendor-list</td>
</tr>
<tr>
<td></td>
<td>display rfdetect vendor-list</td>
</tr>
</tbody>
</table>
clear rfdetect attack-list

Removes a MAC address from the attack list.

**Syntax** — `clear rfdetect attack-list mac-addr`

- `mac-addr` — MAC address you want to remove from the attack list.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command clears MAC address 11:22:33:44:55:66 from the attack list:

```
```
clear rfdetect black-list

Removes a MAC address from the client black list.

Syntax — clear rfdetect black-list mac-addr

- mac-addr — MAC address you want to remove from the black list.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command removes MAC address 11:22:33:44:55:66 from the black list:


See Also
- clear rfdetect attack-list on page 678
- display rfdetect attack-list on page 683
**Examples** — The following command removes BSSID `aa:bb:cc:11:22:33` from the ignore list for RF scans:

```
WX1200# clear rfdetect ignore aa:bb:cc:11:22:33
```

**See Also**
- `display rfdetect ignore` on page 692
- `set rfdetect ignore` on page 704

**clear rfdetect ssid-list**

Removes an SSID from the permitted SSID list.

**Syntax** — `clear rfdetect ssid-list ssid-name`

- `ssid-name` — SSID name you want to remove from the permitted SSID list.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command clears SSID `mycorp` from the permitted SSID list:

```
WX1200# clear rfdetect ssid-list mycorp
success: mycorp is no longer in ssid-list.
```

**See Also**
- `display rfdetect ssid-list` on page 697
- `set rfdetect ssid-list` on page 707
clear rfdetect vendor-list

Removes an entry from the permitted vendor list.

**Syntax** — clear rfdetect vendor-list {client | ap} mac-addr | all

- **client | ap** — Specifies whether the entry is for an AP brand or a client brand.
- **mac-addr | all** — Organizationally Unique Identifier (OUI) to remove.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command removes client OUI aa:bb:cc:00:00:00 from the permitted vendor list:

WX4400# clear rfdetect vendor-list client aa:bb:cc:00:00:00 success: aa:bb:cc:00:00:00 is no longer in client vendor-list.

**See Also**

- [display rfdetect vendor-list](#) on page 697
- [set rfdetect vendor-list](#) on page 708
**rfping**

Provides information about the RF link between the WX and the client based on sending test packets to the client.

- **Syntax** — `rfping {mac mac-addr | session-id session-id}`
  
  - `mac-addr` — Tests the RF link between the WX and the client with the specified MAC address.
  
  - `session-id` — Tests the RF link between the WX and the client with the specified local session ID.

**Defaults** — None.

**Access** — Enabled.

**History** — Version 4.2 Command introduced. Version 6.0 Name of command changed from `test rflink` to `rfping`.

**Usage** — Use this command to send test packets to a specified client. The output of the command indicates the number of test packets received and acknowledged by the client, as well as the client’s signal strength and signal-to-noise ratio.

**Examples** — The following command tests the RF link between the WX switch and the client with MAC address 00:0e:9b:bf:ad:13:

```
WX# rfping mac 00:0e:9b:bf:ad:13
RF-Link Test to 00:0e:9b:bf:ad:13 :
Session-Id: 2
Packets Sent Packets Rcvd RSSI SNR RTT (micro-secs)
------------ ------------ ------- ----- ----------------
20 20 -68 26 976
```

Table 83 describes the fields in this display.

**Table 103**  rfping Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Sent</td>
<td>The number of test packets sent from the WX switch to the client.</td>
</tr>
<tr>
<td>Packets Rcvd</td>
<td>The number of test packets acknowledged by the client.</td>
</tr>
</tbody>
</table>
Table 103  rfping Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSSI</td>
<td>Received signal strength indication (RSSI) of the strength of the RF signal from the client, in decibels referred to 1 milliwatt (dBm).</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-noise ratio (SNR), in decibels (dB), of the data received from the client.</td>
</tr>
<tr>
<td>RTT (micro-secs)</td>
<td>The round-trip time, in microseconds, for the client response to the test packets.</td>
</tr>
</tbody>
</table>

See Also

- display rfdetect data on page 690
- display rfdetect visible on page 698

---

**display rfdetect attack-list**

Displays information about the MAC addresses in the attack list.

**Syntax** — `display rfdetect attack-list`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following example shows the attack list on WX switch:

```
WX1200# display rfdetect attack-list
Total number of entries: 1
  Attacklist MAC    Port/Radio/Chan   RSSI      SSID
  ----------------- ----------------- ------ ------------
```

See Also

- clear rfdetect attack-list on page 678
- set rfdetect attack-list on page 701
display rfdetect black-list

Displays information about the clients in the client black list.

Syntax — display rfdetect black-list

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following example shows the client black list on WX switch:

WX1200# display rfdetect black-list
Total number of entries: 1

<table>
<thead>
<tr>
<th>Blacklist MAC</th>
<th>Type</th>
<th>Port</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:22:33:44:55:66</td>
<td>configured</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>11:23:34:45:56:67</td>
<td>assoc req flood</td>
<td>3</td>
<td>25</td>
</tr>
</tbody>
</table>

See Also

- clear rfdetect black-list on page 679
- set rfdetect black-list on page 702
display rfdetect clients

Displays the wireless clients detected by a WX switch.

Syntax — display rfdetect clients [mac mac-addr]

mac mac-addr — Displays detailed information for a specific client.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Examples — The following command shows information about all wireless clients detected by a WX switch’s MAPs:

WX4400# display rfdetect clients
Total number of entries: 30

<table>
<thead>
<tr>
<th>Client MAC</th>
<th>Client Vendor</th>
<th>AP MAC Vendor</th>
<th>Port/Radio</th>
<th>NoL Type</th>
<th>Last seen</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:03:7f:bf:16:70</td>
<td>Unknown</td>
<td>Unknown</td>
<td>ap 1/1/6</td>
<td>1 intfr</td>
<td>207</td>
</tr>
<tr>
<td>00:04:23:77:e6:e5</td>
<td>Intel</td>
<td>Unknown</td>
<td>ap 1/1/2</td>
<td>1 intfr</td>
<td>155</td>
</tr>
<tr>
<td>00:05:5d:79:ce:0f</td>
<td>D-Link</td>
<td>Unknown</td>
<td>ap 1/1/149</td>
<td>1 intfr</td>
<td>87</td>
</tr>
<tr>
<td>00:05:5d:7e:96:a7</td>
<td>D-Link</td>
<td>Unknown</td>
<td>ap 1/1/149</td>
<td>1 intfr</td>
<td>117</td>
</tr>
<tr>
<td>00:05:5d:7e:96:ce</td>
<td>D-Link</td>
<td>Unknown</td>
<td>ap 1/1/157</td>
<td>1 intfr</td>
<td>162</td>
</tr>
<tr>
<td>00:05:5d:84:d1:c5</td>
<td>D-Link</td>
<td>Unknown</td>
<td>ap 1/1/1</td>
<td>1 intfr</td>
<td>52</td>
</tr>
</tbody>
</table>

The following command displays more details about a specific client:

WX4400# display rfdetect clients mac 00:0c:41:63:fd:6d
Client Mac Address: 00:0c:41:63:fd:6d, Vendor: Linksys
  Port: ap 1, Radio: 1, Channel: 11, RSSI: -82, Rate: 2, Last Seen (secs ago): 84
  Bssid: 00:0b:0e:01:02:00, Vendor: 3Com, Type: intfr, Dst: ff:ff:ff:ff:ff:ff
  Last Rogue Status Check (secs ago): 3

The first line lists information for the client. The other lines list information about the most recent 802.11 packet detected from the client.

Table 104 and Table 105 describe the fields in these displays.
Table 104  display rfdetect clients Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client MAC</td>
<td>MAC address of the client.</td>
</tr>
<tr>
<td>Client Vendor</td>
<td>Company that manufactures or sells the client.</td>
</tr>
<tr>
<td>AP MAC</td>
<td>MAC address of the radio with which the rogue client is associated.</td>
</tr>
<tr>
<td>AP Vendor</td>
<td>Company that manufactures or sells the AP with which the rogue client is associated.</td>
</tr>
<tr>
<td>Port/Radio/Channel</td>
<td>Port number, radio number, and channel number of the radio that detected the rogue.</td>
</tr>
<tr>
<td>NoL</td>
<td>Number of listeners. This is the number of MAP radios that detected the rogue client.</td>
</tr>
<tr>
<td>Type</td>
<td>Classification of the rogue device:</td>
</tr>
<tr>
<td></td>
<td>• rogue—Wireless device that is on the network but is not supposed to be on the network.</td>
</tr>
<tr>
<td></td>
<td>• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios.</td>
</tr>
<tr>
<td></td>
<td>• known—Device that is a legitimate member of the network.</td>
</tr>
<tr>
<td>Last seen</td>
<td>Number of seconds since a MAP radio last detected 802.11 packets from the device.</td>
</tr>
</tbody>
</table>

Table 105  display rfdetect clients mac Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSSI</td>
<td>Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).</td>
</tr>
<tr>
<td>Rate</td>
<td>The data rate of the client.</td>
</tr>
<tr>
<td>Last Seen</td>
<td>Number of seconds since a MAP radio last detected 802.11 packets from the device.</td>
</tr>
<tr>
<td>BSSID</td>
<td>MAC address of the SSID with which the rogue client is associated.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Company that manufactures or sells the AP with which the rogue client is associated.</td>
</tr>
</tbody>
</table>
display rfdetect countermeasures

Displays the current status of countermeasures against rogues in the Mobility Domain.

**Syntax** — `display rfdetect countermeasures`  

**Defaults** — None.

**Access** — Enabled.

**History** — Output no longer lists rogues for which countermeasures have not been started in MSS Version 4.0.

**Usage** — This command is valid only on the seed switch of the Mobility Domain.

**Examples** — The following example displays countermeasures status for the Mobility Domain:

```
WX4400# display rfdetect countermeasures  
Total number of entries: 190  
Rogue MAC   Type  Countermeasures    WX-IPaddr       Port/Radio  
----------------- ----- ------------------ --------------- --------------  
00:0b:0e:00:71:c0 intfr 00:0b:0e:44:55:66 10.1.1.23 ap 4/1/6  
00:0b:0e:03:00:80 rogue 00:0b:0e:11:22:33 10.1.1.23 ap 2/1/11  
```
Table 106 describes the fields in this display.

Table 106  display rfdetect countermeasures Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue MAC</td>
<td>BSSID of the rogue.</td>
</tr>
<tr>
<td>Type</td>
<td>Classification of the rogue device:</td>
</tr>
<tr>
<td></td>
<td>• rogue—Wireless device that is on the network but is not supposed to be on the network.</td>
</tr>
<tr>
<td></td>
<td>• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios.</td>
</tr>
<tr>
<td></td>
<td>• known—Device that is a legitimate member of the network.</td>
</tr>
<tr>
<td>Countermeasures</td>
<td>MAC address of the 3Com radio sending countermeasures against the rogue.</td>
</tr>
<tr>
<td>Radio MAC</td>
<td></td>
</tr>
<tr>
<td>WX-IPaddr</td>
<td>System IP address of the WX switch that is managing the MAP that is sending or will send countermeasures.</td>
</tr>
<tr>
<td>Port/Radio/Channel</td>
<td>Port number, radio number, and channel number of the countermeasures radio.</td>
</tr>
</tbody>
</table>

See Also

- set radio-profile countermeasures on page 458

**display rfdetect counters**

Displays statistics for rogue and Intrusion Detection System (IDS) activity detected by the MAPs managed by a WX switch.

Syntax  —  display rfdetect counters

Defaults  —  None.

Access  —  Enabled.

History  —  Introduced in MSS 4.0.
**Examples** — The following command shows counters for rogue activity detected by a WX switch:

```plaintext
WX4400# display rfdetect counters

<table>
<thead>
<tr>
<th>Type</th>
<th>Current</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue access points</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Interfering access points</td>
<td>139</td>
<td>1116</td>
</tr>
<tr>
<td>Rogue 802.11 clients</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Interfering 802.11 clients</td>
<td>4</td>
<td>347</td>
</tr>
<tr>
<td>802.11 adhoc clients</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Unknown 802.11 clients</td>
<td>20</td>
<td>965</td>
</tr>
<tr>
<td>Interfering 802.11 clients seen on wired network</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 probe request flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 authentication flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 null data flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 mgmt type 6 flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 mgmt type 7 flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 mgmt type d flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 mgmt type e flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 mgmt type f flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 association flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 reassociation flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>802.11 disassociation flood</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Weak wep initialization vectors</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Spoofed access point mac-address attacks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Spoofed client mac-address attacks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Ssid masquerade attacks</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>Spoofed deauthentication attacks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Spoofed disassociation attacks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Null probe responses</td>
<td>626</td>
<td>11380</td>
</tr>
<tr>
<td>Broadcast deauthentications</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FakeAP ssid attacks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FakeAP bssid attacks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Netstumbler clients</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wellenreiter clients</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active scans</td>
<td>1796</td>
<td>4383</td>
</tr>
<tr>
<td>Wireless bridge frames</td>
<td>196</td>
<td>196</td>
</tr>
<tr>
<td>Adhoc client frames</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Access points present in attack-list</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Access points not present in ssid-list</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Access points not present in vendor-list</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Clients not present in vendor-list</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Clients added to automatic black-list</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
**display rfdetect data**

Displays all the BSSIDs detected by an individual WX switch during an RF detection scan. The data includes BSSIDs transmitted by other 3Com radios as well as by third-party access points.

**Syntax** — display rfdetect data

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Vendor, Type, and Flag fields added in MSS Version 4.0.

**Usage** — You can enter this command on any WX switch in the Mobility Domain. The output applies only to the switch on which you enter the command. To display all devices that a specific 3Com radio has detected, even if the radio is managed by another WX switch, use the **display rfdetect visible** command.

To display rogue information for the entire Mobility Domain, use the **display rfdetect mobility-domain** command on the seed switch.

Only one MAC address is listed for each 3Com radio, even if the radio is beaconing multiple SSIDs.

**Examples** — The following command shows the devices detected by this WX switch during the most recent RF detection scan:

```
WX1200# display rfdetect data
Total number of entries: 7

<table>
<thead>
<tr>
<th>BSSID</th>
<th>Port/Rad</th>
<th>Chan</th>
<th>RSSI</th>
<th>Age</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:06:25:09:39:4a</td>
<td>5/1</td>
<td>3</td>
<td>0</td>
<td>15</td>
<td>rack29-hostap</td>
</tr>
<tr>
<td>00:06:25:51:e9:ff</td>
<td>4/1</td>
<td>10</td>
<td>-85</td>
<td>15</td>
<td>Arrow</td>
</tr>
<tr>
<td>00:06:25:51:e9:ff</td>
<td>5/1</td>
<td>10</td>
<td>-84</td>
<td>15</td>
<td>Arrow</td>
</tr>
<tr>
<td>00:0b:0e:00:00:00</td>
<td>4/1</td>
<td>1</td>
<td>-78</td>
<td>15</td>
<td>gary-eng</td>
</tr>
<tr>
<td>00:0b:0e:00:02:00</td>
<td>4/1</td>
<td>11</td>
<td>-76</td>
<td>15</td>
<td>public</td>
</tr>
<tr>
<td>00:0b:0e:00:02:00</td>
<td>5/1</td>
<td>11</td>
<td>-74</td>
<td>15</td>
<td>public</td>
</tr>
<tr>
<td>00:0b:0e:00:02:01</td>
<td>4/1</td>
<td>56</td>
<td>-68</td>
<td>15</td>
<td>public</td>
</tr>
</tbody>
</table>
```

Table 107 describes the fields in this display.
Table 107  display rfdetect data Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>BSSID detected by a MAP radio on this WX switch.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Company that manufactures or sells the rogue device.</td>
</tr>
<tr>
<td>Type</td>
<td>Classification of the rogue device:</td>
</tr>
<tr>
<td></td>
<td>• rogue—Wireless device that is not supposed to be on the network. The device has an entry in a WX switch’s FDB and is therefore on the network.</td>
</tr>
<tr>
<td></td>
<td>• intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a WX switch’s FDB and is not actually on the network, but might be causing RF interference with MAP radios.</td>
</tr>
<tr>
<td></td>
<td>• known—Device that is a legitimate member of the network.</td>
</tr>
<tr>
<td>Port/Radio/Channel</td>
<td>Port number, radio number, and channel number of the radio that detected the rogue.</td>
</tr>
<tr>
<td>Flags</td>
<td>Classification and encryption information for the rogue:</td>
</tr>
<tr>
<td></td>
<td>• The i, a, or u flag indicates the classification.</td>
</tr>
<tr>
<td></td>
<td>• The other flags indicate the encryption used by the rogue.</td>
</tr>
<tr>
<td></td>
<td>For flag definitions, see the key in the command output.</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received signal strength indication (RSSI) — the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm)</td>
</tr>
<tr>
<td>Age</td>
<td>Age of the rogue listing, in seconds. Rogues age out of the rogue list after one minute.</td>
</tr>
<tr>
<td>SSID</td>
<td>Service set identifier (SSID) associated with the BSSID.</td>
</tr>
</tbody>
</table>

See Also

- display rfdetect mobility-domain on page 692
- display rfdetect visible on page 698
CHAPTER 19: RF DETECTION COMMANDS

**display rfdetect ignore**

Displays the BSSIDs of third-party devices that MSS ignores during RF scans. MSS does not generate log messages or traps for the devices in the ignore list.

**Syntax** — `display rfdetect ignore`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — The following example displays the list of ignored devices:

```
WX4400# display rfdetect ignore
Total number of entries: 2
   Ignore MAC
          -----------------
          aa:bb:cc:11:22:33
```

**See Also**

- `clear rfdetect ignore` on page 679
- `set rfdetect ignore` on page 704

**display rfdetect mobility-domain**

Displays the rogues detected by all WX switches in the Mobility Domain during RF detection scans.

**Syntax** — `display rfdetect mobility-domain [ssid ssid-name | bssid mac-addr]`

- `ssid ssid-name` — Displays rogues that are using the specified SSID.
- `bssid mac-addr` — Displays rogues that are using the specified BSSID.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. **Bssid** and **ssid** options added; Vendor, Type and Flag fields added in MSS Version 4.0.
Usage — This command is valid only on the seed switch of the Mobility Domain. To display rogue information for an individual switch, use the display rfdetect data command on that switch.

Only rogues are listed. To display all devices detected, including 3Com radios, use the display rfdetect data command.

Examples — The following example displays information about the BSSIDs detected in the Mobility Domain managed by the seed switch:

```
WX1200# display rfdetect mobility-domain
Total number of entries: 194
Flags: i = infrastructure, a = ad-hoc, u = unresolved
   c = CCMP, t = TKIP, 1 = 104-bit WEP, 4 = 40-bit WEP, w = WEP(non-WPA)
BSSID           Vendor       Type  Flags  SSID
----------------- ------------ ----- ------ --------------------------------
00:07:50:d5:cc:91        Cisco intfr i----w r27-cisco1200-2
00:07:50:d5:dc:78        Cisco intfr i----w r116-cisco1200-2
00:09:b7:7b:8a:54        Cisco intfr i-----
00:0a:5e:4b:4a:c0         3Com intfr i----- public
00:0a:5e:4b:4a:c2         3Com intfr i----w 3Comwlan
00:0a:5e:4b:4a:c4         3Com intfr ic---- 3Com-ccmp
00:0a:5e:4b:4a:c6         3Com intfr i----w 3Com-tkip
00:0a:5e:4b:4a:c8         3Com intfr i----w 3Com-voip
00:0a:5e:4b:4a:ca         3Com intfr i----- 3Com-webaaa
```

The lines in this display are compiled from data from multiple listeners (MAP radios). If an item has the value unresolved, not all listeners agree on the value for that item. Generally, an unresolved state occurs only when a MAP or a Mobility Domain is still coming up, and lasts only briefly.

The following command displays detailed information for rogues using SSID 3com-webaaa.

```
WX1200# display rfdetect mobility-domain ssid 3Com-webaaa
BSSID: 00:0a:5e:4b:4a:ca Vendor: 3Com SSID: 3Com-webaaa
Type: intfr Adhoc: no Crypto-types: clear

WX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/1/11 Mac: 00:0b:6e:00:0a:6a
Device-type: interfering Adhoc: no Crypto-types: clear
RSSI: -85 SSID: 3Com-webaaa

BSSID: 00:0b:0e:00:7a:8a Vendor: 3Com SSID: 3com-webaaa
Type: intfr Adhoc: no Crypto-types: clear
```
Two types of information are shown. The lines that are not indented show the BSSID, vendor, and information about the SSID. The indented lines that follow this information indicate the listeners (MAP radios) that detected the SSID. Each set of indented lines is for a separate MAP listener.

In this example, two BSSIDs are mapped to the SSID. Separate sets of information is shown for each of the BSSIDs, and information about the listeners for each BSSID are shown.

The following command displays detailed information for a BSSID.

```
WX1200# display rfdetect mobility-domain bssid
BSSID: 00:0b:0e:00:4:d1 Vendor: Cisco SSID: notmycorp
Type: rogue Adhoc: no Crypto-types: clear

WX-IPaddress: 10.8.121.102 Port/Radio/Ch: 3/2/56 Mac: 00:0b:0e:00:0a:6b
Device-type: rogue Adhoc: no Crypto-types: clear
RSSI: -72 SSID: notmycorp

WX-IPaddress: 10.3.8.103 Port/Radio/Ch: ap 1/1/157 Mac: 00:0b:0e:76:56:82
Device-type: interfering Adhoc: no Crypto-types: clear
RSSI: -76 SSID: 3Com-webaaa
```
Table 108 and Table 109 describe the fields in these displays.

**Table 108**  
*display rfdetect mobility-domain Output*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>MAC address of the SSID used by the detected device.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Company that manufactures or sells the rogue device.</td>
</tr>
</tbody>
</table>
| **Type** | Classification of the rogue device:  
  - rogue—Wireless device that is not supposed to be on the network. The device has an entry in a WX switch’s FDB and is therefore on the network.  
  - intfr—Wireless device that is not part of your network but is not a rogue. The device does not have an entry in a WX switch’s FDB and is not actually on the network, but might be causing RF interference with MAP radios.  
  - known—Device that is a legitimate member of the network.  
| **Flags** | Classification and encryption information for the rogue:  
  - The i, a, or u flag indicates the classification.  
  - The other flags indicate the encryption used by the rogue. For flag definitions, see the key in the command output. |
| SSID | SSID used by the detected device. |

**Table 109**  
*display rfdetect mobility-domain ssid or bssid Output*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>MAC address of the SSID used by the detected device.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Company that manufactures or sells the rogue device.</td>
</tr>
<tr>
<td>SSID</td>
<td>SSID used by the detected device.</td>
</tr>
</tbody>
</table>
| **Type** | Classification of the rogue device:  
  - rogue—Wireless device that is on the network but is not supposed to be on the network.  
  - intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios.  
  - known—Device that is a legitimate member of the network.  
| **Adhoc** | Indicates whether the rogue is an infrastructure rogue (is using an AP) or is operating in ad-hoc mode. |
Table 109  display rfdetect mobility-domain ssid or bssid Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto-Types</td>
<td>Encryption type:</td>
</tr>
<tr>
<td></td>
<td>clear (no encryption)</td>
</tr>
<tr>
<td></td>
<td>ccmp</td>
</tr>
<tr>
<td></td>
<td>tkip</td>
</tr>
<tr>
<td></td>
<td>wep104 (WPA 104-bit WEP)</td>
</tr>
<tr>
<td></td>
<td>wep40 (WPA 40-bit WEP)</td>
</tr>
<tr>
<td></td>
<td>wep (non-WPA WEP)</td>
</tr>
<tr>
<td>WX-IPaddress</td>
<td>System IP address of the WX switch that detected the rogue.</td>
</tr>
<tr>
<td>Port/Radio/Channel</td>
<td>Port number, radio number, and channel number of the radio that detected the rogue.</td>
</tr>
<tr>
<td>Mac</td>
<td>MAC address of the radio that detected the rogue.</td>
</tr>
<tr>
<td>Device-type</td>
<td>Device type detected by the MAP radio.</td>
</tr>
<tr>
<td>Adhoc</td>
<td>Ad-hoc status (yes or no) detected by the MAP radio.</td>
</tr>
<tr>
<td>Crypto-Types</td>
<td>Encryption type detected by the MAP radio.</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).</td>
</tr>
<tr>
<td>SSID</td>
<td>SSID mapped to the BSSID.</td>
</tr>
</tbody>
</table>

See Also

- display rfdetect data on page 690
- display rfdetect visible on page 698
**display rfdetect ssid-list**

Displays the entries in the permitted SSID list.

**Syntax** — display rfdetect ssid-list

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following example shows the permitted SSID list on WX switch:

```
WX4400# display rfdetect ssid-list
Total number of entries: 3
 SSID
   ------------------
   mycorp
   corporate
   guest
```

**See Also**

- clear rfdetect ssid-list on page 680
- set rfdetect ssid-list on page 707

**display rfdetect vendor-list**

Displays the entries in the permitted vendor list.

**Syntax** — display rfdetect vendor-list

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.
Examples — The following example shows the permitted vendor list on WX switch:

```
WX1200# display rfdetect vendor-list
Total number of entries: 1
  OUI          Type
  ----------------- -----
   aa:bb:cc:00:00:00 client
   11:22:33:00:00:00 ap
```

See Also

- `clear rfdetect vendor-list` on page 681
- `set rfdetect vendor-list` on page 708

**display rfdetect visible**

Displays the BSSIDs discovered by a specific 3Com radio. The data includes BSSIDs transmitted by other 3Com radios as well as by third-party access points.

**Syntax** — `display rfdetect visible mac-addr`

**Syntax** — `display rfdetect visible ap map-num [radio {1 | 2}]`

- `mac-addr` — Base MAC address of the 3Com radio.
  
  *Note:* To display the base MAC address of a 3Com radio, use the `display ap status` command.

- `map-num` — Port connected to the MAP access point for which to display neighboring BSSIDs.

- `dap-num` — Number of a Distributed MAP for which to display neighboring BSSIDs.

- `radio 1` — Shows neighbor information for radio 1.

- `radio 2` — Shows neighbor information for radio 2. (This option does not apply to single-radio models.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
**Usage** — If a 3Com radio is supporting more than one SSID, each of the corresponding BSSIDs is listed separately.

To display rogue information for the entire Mobility Domain, use the display `rfdetect mobility-domain` command on the seed switch.

**Examples** — The following command displays the devices detected by 3Com radio 00:0b:0e:00:0a:6a:

```
WX1200# display rfdetect visible 00:0b:0e:00:0a:6a ap 3 radio 1
```

Total number of entries: 104

<table>
<thead>
<tr>
<th>Transmit MAC</th>
<th>Vendor</th>
<th>Type</th>
<th>Ch</th>
<th>RSSI</th>
<th>Flags</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:07:50:d5:cc:91</td>
<td>Cisco</td>
<td>intfr</td>
<td>6</td>
<td>-60</td>
<td>i----w</td>
<td>r27-cisco1200-2</td>
</tr>
<tr>
<td>00:07:50:d5:dc:78</td>
<td>Cisco</td>
<td>intfr</td>
<td>6</td>
<td>-82</td>
<td>i----w</td>
<td>r116-cisco1200-2</td>
</tr>
<tr>
<td>00:09:b7:7b:8a:54</td>
<td>Cisco</td>
<td>intfr</td>
<td>2</td>
<td>-54</td>
<td>i------</td>
<td></td>
</tr>
<tr>
<td>00:0a:5e:4b:4a:c0</td>
<td>3Com</td>
<td>intfr</td>
<td>11</td>
<td>-57</td>
<td>i------</td>
<td>public</td>
</tr>
<tr>
<td>00:0a:5e:4b:4a:c2</td>
<td>3Com</td>
<td>intfr</td>
<td>11</td>
<td>-82</td>
<td>i-tl--</td>
<td>3Comwlan</td>
</tr>
<tr>
<td>00:0a:5e:4b:4a:c4</td>
<td>3Com</td>
<td>intfr</td>
<td>11</td>
<td>-85</td>
<td>ic----</td>
<td>3com-ccmp</td>
</tr>
<tr>
<td>00:0a:5e:4b:4a:c6</td>
<td>3Com</td>
<td>intfr</td>
<td>11</td>
<td>-85</td>
<td>i--t---</td>
<td>3com-tkip</td>
</tr>
<tr>
<td>00:0a:5e:4b:4a:c8</td>
<td>3Com</td>
<td>intfr</td>
<td>11</td>
<td>-83</td>
<td>i-t---</td>
<td>3com-voip</td>
</tr>
<tr>
<td>00:0a:5e:4b:4a:ca</td>
<td>3Com</td>
<td>intfr</td>
<td>11</td>
<td>-85</td>
<td>i-----</td>
<td>3com-webaaa</td>
</tr>
</tbody>
</table>

Table 110 describes the fields in this display.

**Table 110**  display rfdetect visible Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmit MAC</td>
<td>MAC address the rogue device that sent the 802.11 packet detected by the MAP radio.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Company that manufactures or sells the rogue device.</td>
</tr>
<tr>
<td>Type</td>
<td>Classification of the rogue device:</td>
</tr>
<tr>
<td></td>
<td>• rogue—Wireless device that is on the network but is not supposed to be on the network.</td>
</tr>
<tr>
<td></td>
<td>• intfr—Wireless device that is not part of your network and is not a rogue, but might be causing RF interference with MAP radios.</td>
</tr>
<tr>
<td></td>
<td>• known—Device that is a legitimate member of the network.</td>
</tr>
<tr>
<td>Ch</td>
<td>Channel number on which the radio detected the rogue.</td>
</tr>
</tbody>
</table>
CHAPTER 19: RF DETECTION COMMANDS

set rfdetect active-scan

Disables or reenables active RF detection scanning on a WX switch. When active scanning is enabled, the MAP radios managed by the switch look for rogue devices by sending probe any requests (probe requests with a null SSID name), to solicit probe responses from other access points.

Syntax — set rfdetect active-scan {enable | disable}

- enable — Enables active RF detection scanning.
- disable — Disables active RF detection scanning.

Defaults — Active scanning is enabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — You can enter this command on any WX switch in the Mobility Domain. The command takes effect only on that switch.

Examples — The following command disables active scanning on a WX switch:

WX1200# set rfdetect active-scan disable
success: off-channel scanning is disabled.

See Also
- display rfdetect data on page 690
- display rfdetect mobility-domain on page 692

Table 110 display rfdetect visible Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSSI</td>
<td>Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).</td>
</tr>
<tr>
<td>Flags</td>
<td>Classification and encryption information for the rogue:</td>
</tr>
<tr>
<td></td>
<td>- The i, a, or u flag indicates the classification.</td>
</tr>
<tr>
<td></td>
<td>- The other flags indicate the encryption used by the rogue.</td>
</tr>
<tr>
<td></td>
<td>For flag definitions, see the key in the command output.</td>
</tr>
<tr>
<td>SSID</td>
<td>SSID used by the detected device.</td>
</tr>
</tbody>
</table>

RSSI

Received signal strength indication (RSSI)—the strength of the RF signal detected by the MAP radio, in decibels referred to 1 milliwatt (dBm).

Flags

Classification and encryption information for the rogue:
- The i, a, or u flag indicates the classification.
- The other flags indicate the encryption used by the rogue.
For flag definitions, see the key in the command output.

SSID

SSID used by the detected device.
**set rfdetect attack-list**

Adds an entry to the attack list. The attack list specifies the MAC addresses of devices that MSS should issue countermeasures against whenever the devices are detected on the network. The attack list can contain the MAC addresses of APs and clients.

**Syntax** — `set rfdetect attack-list mac-addr`

- `mac-addr` — MAC address you want to attack.

**Defaults** — The attack list is empty by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — The attack list applies only to the WX switch on which the list is configured. WX switches do not share attack lists.

When on-demand countermeasures are enabled (with the `set radio-profile countermeasures configured` command) only those devices configured in the attack list are subject to countermeasures. In this case, devices found to be rogues by other means, such as policy violations or by determining that the device is providing connectivity to the wired network, are not attacked.

**Examples** — The following command adds MAC address aa:bb:cc:44:55:66 to the attack list:

```
```

**See Also**

- `clear rfdetect attack-list` on page 678
- `display rfdetect attack-list` on page 683
- `set radio-profile countermeasures` on page 458
**set rf detect black-list**

Adds an entry to the client black list. The client black list specifies clients that are not allowed on the network. MSS drops all packets from the clients on the black list.

**Syntax** — `set rfdetect black-list mac-addr`

- `mac-addr` — MAC address you want to place on the black list.

**Defaults** — The client black list is empty by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — In addition to manually configured entries, the list can contain entries added by MSS. MSS can place a client in the black list due to an association, reassociation or disassociation flood from the client.

The client black list applies only to the WX switch on which the list is configured. WX switches do not share client black lists.

**Examples** — The following command adds client MAC address 11:22:33:44:55:66 to the black list:

```
```

**See Also**

- `display rf detect black-list` on page 684
- `set rf detect black-list` on page 702

**set rf detect countermeasures**

Enables or disables countermeasures for the Mobility Domain. Countermeasures are packets sent by a radio to prevent clients from being able to use a rogue access point.

**CAUTION:** Countermeasures affect wireless service on a radio. When a MAP radio is sending countermeasures, the radio is disabled for use by network traffic, until the radio finishes sending the countermeasures.
Syntax — set rfdetect countermeasures {enable | disable}
- enable — Enables countermeasures.
- disable — Disables countermeasures.

Defaults — Countermeasures are disabled by default.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command is valid only on the seed switch of the Mobility Domain.

Examples — The following command enables countermeasures for the Mobility Domain managed by this seed switch:

WX1200# set rfdetect countermeasures enable
success:  countermeasures are now enabled.

See Also
- clear rfdetect attack-list on page 678
- display rfdetect ignore on page 692
- set rfdetect countermeasures mac on page 703

---

**set rfdetect countermeasures mac**

Starts countermeasures against a specific rogue.

Syntax — set rfdetect countermeasures mac mac-addr
- mac-addr — Basic service set identifier (BSSID) of the rogue. Enter the BSSID in MAC address format, using a colon between each octet (for example: aa:bb:cc:dd:ee:ff).

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — Use this command to immediately begin countermeasures against a specific rogue in the rogue list. The MAC address you specify must be in the list of rogues generated by RF detection scans. MSS can issue countermeasures only against a device that is in the rogue list.
You can start countermeasures against more than one BSSID by typing additional `set rfdetect countermeasures mac` commands.

After you type the first `set rfdetect countermeasures mac` command, MSS does not issue countermeasures against any devices except the ones you specify using this command. To resume normal countermeasures operation, where MSS automatically issues countermeasures against detected rogues, use the `clear rfdetect countermeasures mac all` command.

This command is valid only on the seed switch of the Mobility Domain. The countermeasures take effect only if countermeasures are enabled for the Mobility Domain, using the `set rfdetect countermeasures enable` command.

This command does not become part of the configuration file when you save the configuration and therefore is not reloaded if the switch is restarted.

**Examples** — The following command begins countermeasures against rogue BSSID aa:bb:cc:11:22:33:

```
```

**See Also**
- `clear rfdetect attack-list` on page 678
- `display rfdetect ignore` on page 692
- `set rfdetect countermeasures` on page 702

---

**set rfdetect ignore** Configures a list of known devices to ignore during an RF scan. MSS does not generate log messages or traps for the devices in the ignore list.

**Syntax** — `set rfdetect ignore mac-addr`

- `mac-addr` — BSSID (MAC address) of the device to ignore.

**Defaults** — MSS reports all unknown BSSIDs detected during an RF scan.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
Usage — Use this command to identify third-party APs and other devices you are already aware of and do not want MSS to report following RF scans.

If you try to initiate countermeasures against a device on the ignore list, the ignore list takes precedence and MSS does not issue the countermeasures. Countermeasures apply only to rogue devices.

If you add a device that MSS has classified as a rogue to the permitted vendor list or permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list or permitted SSID list merely indicates that the device is from an allowed manufacturer or is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device’s MAC address to the ignore list.

After you add a device that has been classified as a rogue to the ignore list, the device remains classified as a rogue for at least 10 minutes. After 10 minutes, MSS reclassifies the device as an interfering device.

Examples — The following command configures MSS to ignore BSSID aa:bb:cc:11:22:33 during RF scans:


See Also
- clear rfdetect ignore on page 679
- display rfdetect ignore on page 692

set rfdetect log

Disables or reenables generation of log messages when rogues are detected or when they disappear.

Syntax — set rfdetect log {enable | disable}

- enable — Enables logging of rogues.
- disable — Disables logging of rogues.

Defaults — RF detection logging is enabled by default.

Access — Enabled.
**History** — Introduced in MSS Version 3.0.

**Usage** — This command is valid only on the seed switch of the Mobility Domain.

The log messages for rogues are generated only on the seed and appear only in the seed's log message buffer. Use the `display log buffer` command to display the messages in the seed switch's log message buffer.

**Examples** — The following command enables RF detection logging for the Mobility Domain managed by this seed switch:

```
WX1200# set rfdetect log enable
success:  rfdetect logging is enabled.
```

**See Also**

- `display log buffer` on page 760

---

**set rfdetect signature**

Enables MAP signatures. A MAP signature is a set of bits in a management frame sent by a MAP that identifies that MAP to MSS. If someone attempts to spoof management packets from a 3Com MAP, MSS can detect the spoof attempt.

**Syntax** — `set rfdetect signature {enable | disable}`

- `enable` — Enables MAP signatures.
- `disable` — Disables MAP signatures.

**Defaults** — MAP signatures are disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — The command applies only to MAPs managed by the WX switch on which you enter the command. To enable signatures on all MAPs in a Mobility Domain, enter the command on each WX switch in the Mobility Domain.

> You must use the same MAP signature setting (enabled or disabled) on all WX switches in a Mobility Domain.
**set rfdetect signature key**

Creates an encrypted RF fingerprint key to use as a signature for a MAP.

**Syntax** — `set rfdetect signature key encrypted <key_value>`

- **key** — 16 bytes separated by colons generated by the user. For example, `a1:b2:c3:d4:e5:f6:g7:h8` can be a key value.
- **encrypted** — Encrypts the signature key.

**Defaults** — Disabled by default.

**Access** — Enabled

**History** — Introduced in 5.0

---

**set rfdetect ssid-list**

Adds an SSID to the permitted SSID list. The permitted SSID list specifies the SSIDs that are allowed on the network. If MSS detects packets for an SSID that is not on the list, the AP that sent the packets is classified as a rogue. MSS issues countermeasures against the rogue if they are enabled.

**Syntax** — `set rfdetect ssid-list ssid-name`

- **ssid-name** — SSID name you want to add to the permitted SSID list.

**Defaults** — The permitted SSID list is empty by default and all SSIDs are allowed. However, after you add an entry to the list, MSS allows traffic only for the SSIDs that are on the list.

**Access** — Enabled

**History** — Introduced in MSS Version 4.0.

**Usage** — The permitted SSID list applies only to the WX switch on which the list is configured. WX switches do not share permitted SSID lists.

---

**Examples** — The following command enables MAP signatures on a WX switch:

```
WX1200# set rfdetect signature enable
success:  signature is now enabled.
```
If you add a device that MSS has classified as a rogue to the permitted SSID list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted SSID list merely indicates that the device is using an allowed SSID. However, to cause MSS to stop classifying the device as a rogue, you must add the device’s MAC address to the ignore list.

**Examples** — The following command adds SSID `mycorp` to the list of permitted SSIDs:

```
WX1200# set rfdetect ssid-list mycorp
success: ssid mycorp is now in ssid-list.
```

**See Also**

- `clear rfdetect ssid-list` on page 680
- `display rfdetect ssid-list` on page 697

---

**set rfdetect vendor-list**

Adds an entry to the permitted vendor list. The permitted vendor list specifies the third-party AP or client vendors that are allowed on the network. MSS does not list a device as a rogue or interfering device if the device’s OUI is in the permitted vendor list.

**Syntax** — `set rfdetect vendor-list {client | ap} mac-addr`

- `client | ap` — Specifies whether the entry is for an AP brand or a client brand.
- `mac-addr` — Organizationally Unique Identifier (OUI) to remove.

**Defaults** — The permitted vendor list is empty by default and all vendors are allowed. However, after you add an entry to the list, MSS allows only the devices whose OUIs are on the list.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — The permitted vendor list applies only to the WX switch on which the list is configured. WX switches do not share permitted vendor lists.
If you add a device that MSS has classified as a rogue to the permitted vendor list, but not to the ignore list, MSS can still classify the device as a rogue. Adding an entry to the permitted vendor list merely indicates that the device is from an allowed vendor. However, to cause MSS to stop classifying the device as a rogue, you must add the device’s MAC address to the ignore list.

Examples — The following command adds an entry for clients whose MAC addresses start with aa:bb:cc:

WX1200# set rfdetect vendor-list client aa:bb:cc:00:00:00
success: MAC aa:bb:cc:00:00:00 is now in client vendor-list.

The trailing 00:00:00 value is required.

See Also

- clear rfdetect vendor-list on page 681
- display rfdetect vendor-list on page 697

**test rflink**

Provides information about the RF link between the WX switch and the client based on sending test packets to the client.

**Syntax** — `test rflink {mac mac-addr | session-id session-id}

- `mac-addr` — Tests the RF link between the WX switch and the client with the specified MAC address.
- `session-id` — Tests the RF link between the WX switch and the client with the specified local session ID.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

**Usage** — Use the `test rflink` command to send test packets to a specified client. The output of the command indicates the number of test packets received and acknowledged by the client, as well as the client’s signal strength and signal-to-noise ratio.
Examples — The following command tests the RF link between the WX switch and the client with MAC address 00:0e:9b:bf:ad:13:

```
WX4400# test rflink mac 00:0e:9b:bf:ad:13
RF-Link Test to 00:0e:9b:bf:ad:13:
Session-Id: 2
Packets Sent  Packets Rcvd  RSSI     SNR    RTT (micro-secs)
------------  ------------  -------  -----  ----------------
    20            20      -68     26        976
```

Table 111 describes the fields in this display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Sent</td>
<td>The number of test packets sent from the WX switch to the client.</td>
</tr>
<tr>
<td>Packets Rcvd</td>
<td>The number of test packets acknowledged by the client.</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received signal strength indication (RSSI)—the strength of the RF signal from the client, in decibels referred to 1 milliwatt (dBm).</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-noise ratio (SNR), in decibels (dB), of the data received from the client.</td>
</tr>
<tr>
<td>RTT (micro-secs)</td>
<td>The round-trip time, in microseconds, for the client response to the test packets.</td>
</tr>
</tbody>
</table>

See Also

- display rfdetect data on page 690
- display rfdetect visible on page 698
20

**FILE MANAGEMENT COMMANDS**

Use file management commands to manage system files and to display software and boot information.

This chapter presents file management commands alphabetically. Use Table 112 to locate commands in this chapter based on their use.

**Table 112  File Management Commands by Usage**

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Version</td>
<td>reset system</td>
<td>731</td>
</tr>
<tr>
<td></td>
<td>display version</td>
<td>725</td>
</tr>
<tr>
<td>Boot Settings</td>
<td>set boot partition</td>
<td>736</td>
</tr>
<tr>
<td></td>
<td>set boot configuration-file</td>
<td>735</td>
</tr>
<tr>
<td></td>
<td>set boot backup-configuration</td>
<td>734</td>
</tr>
<tr>
<td></td>
<td>display boot</td>
<td>722</td>
</tr>
<tr>
<td></td>
<td>clear boot config</td>
<td>714</td>
</tr>
<tr>
<td></td>
<td>clear boot backup-configuration</td>
<td>714</td>
</tr>
<tr>
<td>File Management</td>
<td>dir</td>
<td>718</td>
</tr>
<tr>
<td></td>
<td>copy</td>
<td>715</td>
</tr>
<tr>
<td></td>
<td>md5</td>
<td>729</td>
</tr>
<tr>
<td></td>
<td>delete</td>
<td>717</td>
</tr>
<tr>
<td></td>
<td>mkdir</td>
<td>729</td>
</tr>
<tr>
<td></td>
<td>rmdir</td>
<td>733</td>
</tr>
<tr>
<td>Configuration File</td>
<td>save config</td>
<td>733</td>
</tr>
<tr>
<td></td>
<td>load config</td>
<td>727</td>
</tr>
<tr>
<td></td>
<td>display config</td>
<td>723</td>
</tr>
</tbody>
</table>
CHAPTER 20: FILE MANAGEMENT COMMANDS

Table 112  File Management Commands by Usage (continued)

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Backup and Restore</td>
<td>backup on page 712</td>
</tr>
<tr>
<td></td>
<td>restore on page 732</td>
</tr>
<tr>
<td>Sygate On-Demand Agent (SODA) file installation and removal</td>
<td>install soda agent on page 721</td>
</tr>
<tr>
<td></td>
<td>display boot on page 722</td>
</tr>
</tbody>
</table>

backup

Creates an archive of WX system files and optionally, user file, in Unix tape archive (tar) format.

Syntax — backup system [tftp:/ip-addr/]filename [all | critical]

Defaults — All.

Access — Enabled.

History —

Usage — You can create an archive located on a TFTP server or in the switch's nonvolatile storage. If you specify a TFTP server as part of the filename, the archive is copied directly to the TFTP server and not stored locally on the switch.

Use the critical option if you want to back up or restore only the system-critical files required to operate and communicate with the switch. Use the all option if you also want to back up or restore WebAAA pages, backup configuration files, image files, and any other files stored in the user files area of nonvolatile storage.

The maximum supported file size is 32 MB. If the file size of the tarball is too large, delete unnecessary files (such as unneeded copies of system image files) and try again, or use the critical option instead of the all option.

Neither option archives image files or any other files listed in the Boot section of dir command output. The all option archives image files only if they are present in the user files area.
Archive files created by the `all` option are larger than files created by the `critical` option. The file size depends on the files in the user area, and the file can be quite large if the user area contains image files.

The `backup` command places the boot configuration file into the archive. (The boot configuration file is the `configured boot configuration` in the `display boot` command’s output.) If the running configuration contains changes that have not been saved, these changes are not in the boot configuration file and are not archived. To make sure the archive contains the configuration that is currently running on the switch, use the `save config` command to save the running configuration to the boot configuration file, before using the `backup` command.

**Examples** — The following command creates an archive of the system-critical files and copies the archive directly to a TFTP server. The filename in this example includes a TFTP server IP address, so the archive is not stored locally on the switch.

```
WX1200# backup system tftp:/10.10.20.9/sysa_bak critical
success: sent 28263 bytes in 0.324 seconds [ 87231 bytes/sec]
```

Table 113 describes the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tftp://ip</code></td>
<td>Name of the archive file to create. You can store the file locally in the</td>
</tr>
<tr>
<td><code>-addr/filen</code></td>
<td>switch’s nonvolatile storage or on a TFTP server.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Backs up system files and all the files in the user files area.</td>
</tr>
<tr>
<td></td>
<td>The user files area contains the set of files listed in the <code>file</code> section</td>
</tr>
<tr>
<td></td>
<td>of <code>dir</code> command output.</td>
</tr>
<tr>
<td><code>critical</code></td>
<td>Backs up system files only, including the configuration file used when</td>
</tr>
<tr>
<td></td>
<td>booting, and certificate files. The size of an archive created by this</td>
</tr>
<tr>
<td></td>
<td>option is generally 1MB or less.</td>
</tr>
</tbody>
</table>

**See Also**

- `dir` on page 718
- `restore` on page 732
clear boot backup-configuration

Clears the filename specified as the backup configuration file. In the event that MSS cannot read the configuration file at boot time, a backup configuration file is not used.

Syntax — clear boot backup-configuration

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.1.

Examples — The following command clears the name specified as the backup configuration file from the configuration of the WX switch:

WX4400# clear boot backup-configuration
success: Backup boot config filename was cleared.

See Also

• display boot on page 722
• set boot backup-configuration on page 734

clear boot config

Resets to the factory default the configuration that MSS loads during a reboot.

Syntax — clear boot config

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following commands back up the configuration file on a WX switch, reset the switch to its factory default configuration, and reboot the switch:

WX4400# copy configuration tftp://10.1.1.1/backupcfg
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
WX4400# clear boot config
success: Reset boot config to factory defaults.
Perform the following copy operations:

- Copies a file from a TFTP server to nonvolatile storage.
- Copies a file from nonvolatile storage or temporary storage to a TFTP server.
- Copies a file from one area in nonvolatile storage to another.
- Copies a file to a new filename in nonvolatile storage.

Syntax — copy source-url destination-url

- source-url — Name and location of the file to copy. The uniform resource locator (URL) can be one of the following:
  - [subdirname/]filename
  - file:[subdirname/]filename
  - tftp://ip-addr/[subdirname/]filename
  - tmp:filename

For the filename, specify between 1 and 128 alphanumeric characters, with no spaces. Enter the IP address in dotted decimal notation. The subdirname/ option specifies a subdirectory.

- destination-url — Name of the copy and the location where to place the copy. The URL can be one of the following:
  - [subdirname/]filename
  - file:[subdirname/]filename
  - tftp://ip-addr/[subdirname/]filename

If you are copying a system image file into nonvolatile storage, the filename must include the boot partition name. You can specify one of the following:

- boot0:/filename
- boot1:/filename
Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The filename and file:filename URLs are equivalent. You can use either URL to refer to a file in an WX switch’s nonvolatile memory. The tftp://ip-addr/filename URL refers to a file on a TFTP server. If DNS is configured on the WX switch, you can specify a TFTP server’s hostname as an alternative to specifying the IP address.

The tmp:filename URL specifies a file in temporary storage. You can copy a file out of temporary storage but you cannot copy a file into temporary storage. Temporary storage is reserved for use by MSS.

If you are copying a system image file into nonvolatile storage, the filename must be preceded by the boot partition name, which can be boot0 or boot1. Enter the filename as boot0://filename or boot1://filename. You must specify the boot partition that was not used to load the currently running image.

The maximum supported file size for TFTP is 32 MB.

Examples — The following command copies a file called floorwx from nonvolatile storage to a TFTP server:

```
WX4400# copy floorwx tftp://10.1.1.1/floorwx
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
```

The following command copies a file called closetwx from a TFTP server to nonvolatile storage:

```
WX4400# copy tftp://10.1.1.1/closetwx closetwx
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

The following command copies system image WXA03001.Rel from a TFTP server to boot partition 1 in nonvolatile storage:

```
WX4400# copy tftp://10.1.1.107/WXA03001.Rel boot1:WXA03001.Rel
............................................................
................................................success:
received 9163214 bytes in 105.939 seconds [ 86495 bytes/sec]`
The following commands rename `test-config` to `new-config` by copying it from one name to the other in the same location, then deleting `test-config`:

```plaintext
WX4400# copy test-config new-config
WX4400# delete test-config
success: file deleted.
```

The following command copies file `corpa-login.html` from a TFTP server into subdirectory `corpa` in a WX switch's nonvolatile storage:

```plaintext
WX4400# copy tftp://10.1.1.1/corpa-login.html corpa/corpa-login.html
success: received 637 bytes in 0.253 seconds [ 2517 bytes/sec]
```

See Also

- `delete` on page 717
- `dir` on page 718

---

**delete**

Deletes a file.

**CAUTION:** MSS does not prompt you to verify whether you want to delete a file. When you press Enter after typing a `delete` command, MSS immediately deletes the specified file.

MSS does not allow you to delete the currently running software image file or the running configuration.

**Syntax** — `delete url`

- `url` — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

  If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: `subdir_a/file_a`

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — You might want to copy the file to a TFTP server as a backup before deleting the file.
Examples — The following commands copy file testconfig to a TFTP server and delete the file from nonvolatile storage:

WX4400# copy testconfig tftp://10.1.1.1/testconfig
success: sent 365 bytes in 0.401 seconds [ 910 bytes/sec]
WX4400# delete testconfig
success: file deleted.

The following commands delete file dang_doc from subdirectory dang:

WX4400# delete dang/dang_doc
success: file deleted.

See Also

- copy on page 715
- dir on page 718

**dir**

Displays a list of the files in nonvolatile storage and temporary files.

**Syntax**

```
dir [subdirname] [file:] | [core:] | [boot0:] | [boot1:]
```

- **subdirname** — Subdirectory name. If you specify a subdirectory name, the command lists the files in that subdirectory. Otherwise, the command lists the files in the root directory and also lists the subdirectories.
- **file** — Limits dir output to the contents of the user files area.
- **core:** — Limits dir output to the contents of the /tmp/core subdirectory.
- **boot0:** — Limits dir output to the contents of the boot0 partition.
- **boot1:** — Limits dir output to the contents of the boot1 partition

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Core; file; boot0 and boot1 options added, to limit the output to the specified category, in MSS Version 4.0.
Examples — The following command displays the files in the root directory:

WX4400# dir
===============================================================================
file: Filename                                        Size           Created
file:configuration                              48 KB      Jul 12 2005, 15:02:32
corp_a/                                       512 bytes   May 21 2004, 19:15:48
old/                                          512 bytes   May 16 2004, 17:23:44
file:pubsconfig-april062005                     40 KB      May 09 2005, 21:08:30
file:testback                                  28 KB      Apr 19 2005, 16:37:18
Total:         159 Kbytes used, 207663 Kbytes free
===============================================================================
Boot: Filename                                        Size           Created
boot0:wx040100.020                                 9780 KB      Aug 23 2005, 15:54:08
Boot0: Total:        9780 Kbytes used, 2460 Kbytes free
Boot1: Total:        9796 Kbytes used, 2464 Kbytes free
===============================================================================
temporary files: Filename                                        Size           Created
Total:          37 bytes used, 91707 Kbytes free
===============================================================================

The following command displays the files in the old subdirectory:

WX4400# dir old
===============================================================================
file: Filename                                        Size           Created
Total:          27 Kbytes used, 207824 Kbytes free
The following command limits the output to the contents of the user files area:

WX4400# dir file:

```
===============================================================================
file: Filename                                        Size           Created
file:configuration                              48 KB      Jul 12 2005, 15:02:32
corp_a/                                          512 bytes   May 21 2004, 19:15:48
dangdir/                                        512 bytes   May 16 2004, 17:23:44
file:pubsconfig-april062005                       40 KB      May 09 2005, 21:08:30
file:testback                                    28 KB      Apr 19 2005, 16:37:18
Total:         159 Kbytes used, 207663 Kbytes free
```

The following command limits the output to the contents of the /tmp/core subdirectory:

WX4400# dir core:

```
===============================================================================
file: Filename                                        Size           Created
Total:          37 bytes used, 91707 Kbytes free
```

The following command limits the output to the contents of the boot0 partition:

WX4400# dir boot0:

```
===============================================================================
file: Filename                                        Size           Created
boot0:wx040100.020                                    9780 KB     Aug 23 2005, 15:54:08
Total:        9780 Kbytes used, 207663 Kbytes free
```

Table 114 describes the fields in the `dir` output.
install soda agent

Installs Sygate On-Demand (SODA) agent files in a directory on the WX switch.

**Syntax**

```
install soda agent agent-file agent directory
```

- **agent-file** — Name of a .zip file on the WX switch containing SODA agent files.
- **directory** — Directory on the WX switch where SODA agent files are to be installed. The command automatically creates this directory.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.2.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Filename or subdirectory name. For files, the directory name is shown in</td>
</tr>
<tr>
<td></td>
<td>front of the filename (for example, file:configuration). The file: directory is</td>
</tr>
<tr>
<td></td>
<td>the root directory. For subdirectories, a forward slash is shown at the end</td>
</tr>
<tr>
<td></td>
<td>of the subdirectory name (for example, old/). In the boot partitions list</td>
</tr>
<tr>
<td></td>
<td>(Boot:), an asterisk (*) indicates the boot partition from which the currently</td>
</tr>
<tr>
<td></td>
<td>running image was loaded and the image filename.</td>
</tr>
<tr>
<td>Size</td>
<td>Size in Kbytes or bytes.</td>
</tr>
<tr>
<td>Created</td>
<td>System time and date when the file was created or copied onto the switch.</td>
</tr>
<tr>
<td>Total</td>
<td>Number of kilobytes in use to store files and the number that are still free.</td>
</tr>
</tbody>
</table>

**See Also**

- *copy on page 715*
- *delete on page 717*
Usage — The install soda agent command installs a .zip file containing SODA agent files into a directory on the WX switch. Prior to installing the SODA agent files, you must have already copied the .zip file to the WX switch. This command creates the specified directory, unzips the file and places the contents into the directory. If the specified directory has the same name as a service profile, then that service profile uses the SODA agent files in the directory if SODA functionality is enabled for the service profile.

Examples — The following command installs the contents of the file soda.ZIP into a directory called sp1.

WX4400# install soda agent soda.ZIP agent-directory sp1
This command may take up to 20 seconds...

See Also
- display boot on page 722
- set service-profile soda mode on page 510

---

display boot

Displays the system image and configuration filenames used after the last reboot and configured for use after the next reboot.

Syntax — display boot

Defaults — None.

Access — Access.


Examples — The following command shows the boot information for a WX switch:

WX1200# display boot
Configured boot version: 4.1.0.65
Configured boot image: boot1:wx040100.020
Configured boot configuration: file:configuration
Backup boot configuration: file:backup.cfg
Booted version: 4.1.0.65
Booted image: boot1:wx040100.020
Booted configuration: file:configuration
Product model: WX
Table 115 describes the fields in the **display boot** output.

### Table 115  Output for display boot

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configured boot version</td>
<td>Software version the switch will run next time the software is rebooted.</td>
</tr>
<tr>
<td>Configured boot image</td>
<td>Boot partition and image filename MSS will use to boot next time the software is rebooted.</td>
</tr>
<tr>
<td>Configured boot configuration</td>
<td>Configuration filename MSS will use to boot next time the software is rebooted.</td>
</tr>
<tr>
<td>Backup boot configuration</td>
<td>The name of the configuration file to be used in the event that MSS cannot read the configured boot configuration file next time the software is rebooted.</td>
</tr>
<tr>
<td>Booted version</td>
<td>Software version the switch is running.</td>
</tr>
<tr>
<td>Booted image</td>
<td>Boot partition and image filename MSS used the last time the software was rebooted. MSS is running this software image.</td>
</tr>
<tr>
<td>Booted configuration</td>
<td>Configuration filename MSS used to load the configuration the last time the software was rebooted.</td>
</tr>
</tbody>
</table>

**See Also**

- **display version** on page 725
- **reset system** on page 731
- **set boot configuration-file** on page 735

---

**display config**

Displays the configuration running on the WX.

**Syntax** — **display config** [area area] [all]

- **area area** — Configuration area. You can specify one of the following:
  - aaa
  - acls
  - ap
  - arp
  - eapol
  - httpd
  - ip
- ip-config
- l2acl
- log
- mobility-domain
- network-domain
- ntp
- portconfig
- port-group
- qos
- radio-profile
- rfdetect
- service-profile
- sm
- snmp
- snoop
- spantree
- system
- trace
- vlan
- vlan-fdb
- vlan-profile

If you do not specify a configuration area, nondefault information for all areas is displayed.

- all — Includes configuration items that are set to their default values.

 Defaults — None.

 Access — Enabled.

 History — Introduced in MSS Version 3.0. New options added for remote traffic monitoring (snoop) and rfdevice changed to rfdetect in MSS Version 4.0. Version 4.1 added new options l2acl, network-domain, and qos. Version 4.2 changed the portgroup to port-group for consistency with clear port-group, set port-group, and display port-group commands.
**Usage** — If you do not use one of the optional parameters, configuration commands that set nondefault values are displayed for all configuration areas. If you specify an area, commands are displayed for that area only. If you use the **all** option, the display also includes commands for configuration items that are set to their default values.

**Examples** — The following command shows configuration information for VLANs:

```
WX4400# display config area vlan
# Configuration nvgen’d at 2004-5-21 19:36:48
# Image 3.0.0
# Model WX4400
# Last change occurred at 2004-5-21 18:20:50
set vlan 1 port 1
```

**See Also**
- `load config` on page 727
- `save config` on page 733

---

**display version**

Displays software and hardware version information for an WX switch and, optionally, for any attached MAP access points.

**Syntax** — `display version [details]`

- `details` — Includes additional software build information and information about the MAP access points configured on the WX switch.

**Defaults** — None

**Access** — All.

**History** — Introduced in MSS Version 3.0.
Examples — The following command displays version information for a WX switch:

WX1200# display version

Mobility System Software, Version: 4.1.0 QA 67
Copyright (c) 2002, 2003, 2004, 2005 3Com Corporation. All rights reserved.

Build Information: (build#67) TOP 2005-07-21 04:41:00
Model: WX
Hardware
Mainboard: version 24 ; revision 3 ; FPGA version 24
PoE board: version 1 ; FPGA version 6
Serial number 0321300013
Flash: 4.1.0.14 - md0a
Kernel: 3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader: 4.10 / 4.1.0

The following command displays additional software build information and MAP access point information:

WX1200# display version details

Mobility System Software, Version: 4.1.0 QA 67
Copyright (c) 2002, 2003, 2004, 2005 3Com Corporation. All rights reserved.

Build Information: (build#67) TOP 2005-07-21 04:41:00
Label: 4.1.0.67_072105_WX20
Build Suffix: -d-01
Model: WX
Hardware
Mainboard: version 24 ; revision 3 ; FPGA version 24
CPU Model: 750 (Revision 3.1)
PoE board: version 1 ; FPGA version 6
Serial number 0321300013
Flash: 4.1.0.14 - md0a
Kernel: 3.0.0#20: Fri May 20 17:43:51 PDT 2005
BootLoader: 4.10 / 4.1.0

Port/ AP AP Model Serial # Versions
--------- ------------ ------------
11  /-AP3750 0424902948 H/W : A

F/W1 : 5.6
F/W2 : 5.6
S/W : 4.1.0.67_072105_0432__AP
BOOT S/W : 4.0.3.15_062705_0107__AP
Table 116 describes the fields in the display version output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build Information</td>
<td>Factory timestamp of the image file.</td>
</tr>
<tr>
<td>Label</td>
<td>Software version and build date.</td>
</tr>
<tr>
<td>Build Suffix</td>
<td>Build suffix.</td>
</tr>
<tr>
<td>Model</td>
<td>Build model.</td>
</tr>
<tr>
<td>Hardware</td>
<td>Version information for the WX switch’s motherboard and Power over Ethernet (PoE) board.</td>
</tr>
<tr>
<td>Serial number</td>
<td>Serial number of the WX switch.</td>
</tr>
<tr>
<td>Flash</td>
<td>Flash memory version.</td>
</tr>
<tr>
<td>Kernel</td>
<td>Kernel version.</td>
</tr>
<tr>
<td>BootLoader</td>
<td>Boot code version.</td>
</tr>
<tr>
<td>Port/AP</td>
<td>Port number connected to a MAP access point.</td>
</tr>
<tr>
<td>AP Model</td>
<td>MAP model number.</td>
</tr>
<tr>
<td>Serial #</td>
<td>MAP serial number.</td>
</tr>
<tr>
<td>Versions</td>
<td>MAP hardware, firmware, and software versions.</td>
</tr>
</tbody>
</table>

See Also

- display boot on page 722

**load config**

Loads configuration commands from a file and replaces the WX switch’s running configuration with the commands in the loaded file.

**CAUTION:** This command completely removes the running configuration and replaces it with the configuration contained in the file. 3Com recommends that you save a copy of the current running configuration to a backup configuration file before loading a new configuration.

**Syntax** — `load config [url]`

- **url** — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.

  If the file is in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: `backup_configs/config_c`
Defaults — The default file location is nonvolatile storage.

The current version supports loading a configuration file only from the switch’s nonvolatile storage. You cannot load a configuration file directly from a TFTP server.

If you do not specify a filename, MSS uses the same configuration filename that was used for the previous configuration load. For example, if the WX switch used configuration for the most recent configuration load, MSS uses configuration again unless you specify a different filename. To display the filename of the configuration file MSS loaded during the last reboot, use the display boot command.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — This command completely replaces the running configuration with the configuration in the file.

Examples — The following command reloads the configuration from the most recently loaded configuration file:

WX4400# load config
Reloading configuration may result in lost of connectivity, do you wish to continue? (y/n) [n]y
success: Configuration reloaded

The following command loads configuration file testconfig1:

WX4400# load config testconfig1
Reloading configuration may result in lost of connectivity, do you wish to continue? (y/n) [n]y
success: Configuration reloaded

See Also
- display boot on page 722
- display config on page 723
- save config on page 733
**md5**

Calculates the MD5 checksum for a file in the switch’s nonvolatile storage.

**Syntax**

`md5 [boot0: | boot1:]filename`

- **boot0:** | **boot1:** — Boot partition into which you copied the file.
- **filename** — Name of the file.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — You must include the boot partition name in front of the filename. If you specify only the filename, the CLI displays a message stating that the file does not exist.

**Examples** — The following command calculates the checksum for image file WX040003.020 in boot partition 0:

```
pubs# md5 boot0:WX040003.020
MD5 (boot0:WX040003.020) = b9cf7f527f74608e50c70e8fb896392a
```

**See Also**

- `copy` on page 715
- `dir` on page 718

---

**mkdir**

Creates a new subdirectory in nonvolatile storage.

**Syntax**

`mkdir [subdirname]`

- **subdirname** — Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
Examples — The following commands create a subdirectory called corp2 and display the root directory to verify the result:

WX4400# mkdir corp2
success: change accepted.
WX4400# dir
===============================================================================
file:                          Size     Created
file:configuration             17 KB   May 21 2004, 18:20:53
corp_a/                       512 bytes May 21 2004, 19:15:48
file:dangcfg                  13 KB   May 16 2004, 18:30:44
dangdir/                      512 bytes May 16 2004, 17:23:44
old/                          512 bytes Sep 23 2003, 21:58:48
Total:                         33 Kbytes used, 207822 Kbytes free
===============================================================================
Boot:                          Size     Created
*boot0:bload                   746 KB   May 09 2004, 19:02:16
*boot0:WXA03002.Rel            8182 KB  May 09 2004, 18:58:16
boot1:WXA03001.Rel             8197 KB  May 21 2004, 18:01:02
Boot0: Total:                 8928 Kbytes used, 3312 Kbytes free
Boot1: Total:                  8197 Kbytes used, 4060 Kbytes free
===============================================================================
temporary files:
Filename                             Size     Created
Total:                                0 bytes used, 93537 Kbytes free

See Also
- dir on page 718
- rmdir on page 733
reset system

Restarts an WX switch and reboots the software.

Syntax — reset system [force]

- force — Immediately restarts the system and reboots, without comparing the running configuration to the configuration file.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — If you do not use the force option, the command first compares the running configuration to the configuration file. If the running configuration and configuration file do not match, MSS does not restart the WX switch but instead displays a message advising you to either save the configuration changes or use the force option.

Examples — The following command restarts an WX switch that does not have any unsaved configuration changes:

WX4400# reset system
This will reset the entire system. Are you sure (y/n)y

The following commands attempt to restart an WX switch with a running configuration that has unsaved changes, and then force the switch to restart:

WX4400# reset system
error: Cannot reset, due to unsaved configuration changes.
Use "reset system force" to override.
WX4400# reset system force
...... rebooting ......

See Also
- display boot on page 722
- display version on page 725
- save config on page 733
**restore**

Unzips a system archive created by the backup command and copies the files from the archive onto the switch.

**Syntax**

```
restore system [tftp:/ip-addr/]filename [all | critical]
```

**Defaults** — Critical.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.2.

**Usage** — If a file in the archive has a counterpart on the switch, the archive version of the file replaces the file on the switch. The restore command does not delete files that do not have counterparts in the archive. For example, the command does not completely replace the user files area. Instead, files in the archive are added to the user files area. A file in the user area is replaced only if the archive contains a file with the same name.

**Note:** If the archive’s files cannot fit on the switch, the restore operation fails. 3Com recommends deleting unneeded image files before creating or restoring an archive.

The **backup** command stores the MAC address of the switch in the archive. By default, the **restore** command works only if the MAC address in the archive matches the MAC address of the switch where the **restore** command is entered. The **force** option overrides this restriction and allows you to unpack one switch’s archive onto another switch.

**CAUTION:** Do not use the force option unless you are certain you want to replace the switch’s files with files from another switch. If you restore one switch’s system files onto another switch, you must generate new key pairs and certificates on the switch.

**Examples** — The following command restores system-critical files on a switch, from archive sysa_bak.

```
WX1200# restore system tftp:/10.10.20.9/sysa_bak
success: received 11908 bytes in 0.150 seconds [ 79386 bytes/sec]
success: restore complete.
```
See Also

- backup on page 712

**rmdir**

Removes a subdirectory from nonvolatile storage.

**Syntax** — `rmdir [subdirname]`

- **subdirname** — Subdirectory name. Specify between 1 and 32 alphanumeric characters, with no spaces.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — MSS does not allow the subdirectory to be removed unless it is empty. Delete all files from the subdirectory before attempting to remove it.

**Examples** — The following example removes subdirectory corp2:

```
WX4400# rmdir corp2
success: change accepted.
```

See Also

- **dir** on page 718
- **mkdir** on page 729

**save config**

Saves the running configuration to a configuration file.

**Syntax** — `save config [filename]`

- **filename** — Name of the configuration file. Specify between 1 and 128 alphanumeric characters, with no spaces.

  To save the file in a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example:

  `backup_configs/config_c`

**Defaults** — By default, MSS saves the running configuration as the configuration filename used during the last reboot.
**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — If you do not specify a filename, MSS replaces the configuration file loaded during the most recent reboot. To display the filename of the configuration file MSS loaded during the most recent reboot, use the `display boot` command.

The command completely replaces the specified configuration file with the running configuration.

**Examples** — The following command saves the running configuration to the configuration file loaded during the most recent reboot. In this example, the filename used during the most recent reboot is `configuration`.

```
WX4400# save config
Configuration saved to configuration.
```

The following command saves the running configuration to a file named `testconfig1`:

```
WX4400# save config testconfig1
Configuration saved to testconfig1.
```

**See Also**

- `display boot` on page 722
- `display config` on page 723
- `load config` on page 727

---

**set boot backup-configuration**

Specifies the name of a backup configuration file to be used in the event that MSS cannot read the WX switch’s configuration file at boot time.

**Syntax** — `set boot backup-configuration filename`

- `filename` — Name of the file to use as a backup configuration file if MSS cannot read the WX switch’s configuration file.

**Defaults** — By default, there is no backup configuration file.

**Access** — Enabled.
History — Introduced in MSS Version 4.1.

Examples — The following command specifies a file called backup.cfg as the backup configuration file on the WX switch:

WX1200# set boot backup-configuration backup.cfg
  success: backup boot config filename set.

See Also

- clear boot backup-configuration on page 714
- display boot on page 722

set boot configuration-file

Changes the configuration file to load after rebooting.

Syntax — set boot configuration-file filename

- filename — Filename. Specify between 1 and 128 alphanumeric characters, with no spaces.
  To load the file from a subdirectory, specify the subdirectory name, followed by a forward slash, in front of the filename. For example: backup_configs/config_c.

Defaults — The default configuration filename is configuration.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Usage — The file must be located in the switch's nonvolatile storage.

Examples — The following command sets the boot configuration file to testconfig1:

WX4400# set boot configuration-file testconfig1
  success: boot config set.
**set boot partition**

Specifies the boot partition in which to look for the system image file following the next system reset, software reload, or power cycle.

**Syntax** — `set boot partition {boot0 | boot1}`
- **boot0** — Boot partition 0.
- **boot1** — Boot partition 1.

**Defaults** — By default, an WX switch uses the same boot partition for the next software reload that was used to boot the currently running image.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — To determine the boot partition that was used to load the currently running software image, use the `dir` command.

**Examples** — The following command sets the boot partition for the next software reload to partition 1:

```
WX4400# set boot partition boot1
success: Boot partition set to boot1.
```

**See Also**
- `copy` on page 715
- `dir` on page 718
- `reset system` on page 731

---

**uninstall soda agent**

Removes the contents of a directory containing SODA agent files.

**Syntax** — `uninstall soda agent agent-directory directory`
- **directory** — Directory on the WX switch where soda agent files are to be removed.

**Defaults** — None.

**Access** — Enabled.

**History** — MSS Version 4.2.
Usage — The **uninstall soda command** removes the SODA agent directory and all of its contents. All files in the specified directory are removed. The command removes the directory and its contents, regardless of whether it contains SODA agent files.

Examples — The following command removes the directory *sp1* and all of its contents:

```
WX4400# uninstall soda agent agent-directory sp1
```

This will delete all files in agent-directory, do you wish to continue? (y|n) [n]y

See Also
- **install soda agent** on page 721
- **set service-profile soda mode** on page 510
trace commands

Use trace commands to perform diagnostic routines. While MSS allows you to run many types of traces, this chapter describes commands for those traces you are most likely to use. For a complete listing of the types of traces MSS allows, type the `set trace ?` command.

**CAUTION:** Using the `set trace` command can have adverse effects on system performance. 3Com recommends that you use the lowest levels possible for initial trace commands, and slowly increase the levels to get the data you need.

This chapter presents trace commands alphabetically. Use Table 117 to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace</td>
<td><code>set trace sm</code></td>
<td>745</td>
</tr>
<tr>
<td></td>
<td><code>set trace dot1x</code></td>
<td>744</td>
</tr>
<tr>
<td></td>
<td><code>set trace authentication</code></td>
<td>742</td>
</tr>
<tr>
<td></td>
<td><code>set trace authorization</code></td>
<td>743</td>
</tr>
<tr>
<td></td>
<td><code>display trace</code></td>
<td>741</td>
</tr>
<tr>
<td></td>
<td><code>save trace</code></td>
<td>742</td>
</tr>
<tr>
<td></td>
<td><code>clear trace</code></td>
<td>740</td>
</tr>
<tr>
<td></td>
<td><code>clear log trace</code></td>
<td>740</td>
</tr>
</tbody>
</table>
clear log trace

Deletes the log messages stored in the trace buffer.

**Syntax** — clear log trace

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To delete the trace log, type the following command:

WX4400# clear log trace

**See Also**

- display log buffer on page 760
- set log on page 764

---

clear trace

Deletes running trace commands and ends trace processes.

**Syntax** — clear trace {trace-area | all}

- **trace-area** — Ends a particular trace process. Specify one of the following keywords to end the traces documented in this chapter:
  - **authorization** — Ends an authorization trace
  - **dot1x** — Ends an 802.1X trace
  - **authentication** — Ends an authentication trace
  - **sm** — Ends a session manager trace
  - **all** — Ends all trace processes.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To clear all trace processes, type the following command:

WX4400# clear trace all

success: clear trace all
To clear the session manager trace, type the following command:

```
WX4400# clear trace sm
success: clear trace sm
```

See Also

- `display trace` on page 741
- `set trace authentication` on page 742
- `set trace authorization` on page 743
- `set trace dot1x` on page 744
- `set trace sm` on page 745

---

display trace

Displays information about traces that are currently configured on the WX switch, or all possible trace options.

Syntax — `display trace [all]`

- **all** — Displays all possible trace options and their configuration.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To view the traces currently running, type the following command:

```
WX4400# display trace
milliseconds spent printing traces: 1885.614
Trace Area    Level   Mac               User              Port Filter
-------------- -------- ----------------- ----------------- ---- --------
dot1x          5       ---------------             0
sm             5       ---------------             0
```

See Also

- `clear trace` on page 740
- `set trace authentication` on page 742
- `set trace authorization` on page 743
- `set trace dot1x` on page 744
- `set trace sm` on page 745
**save trace**

Saves the accumulated trace data for enabled traces to a file in the WX switch’s nonvolatile storage.

**Syntax** — save trace filename

- *filename* — Name for the trace file. To save the file in a subdirectory, specify the subdirectory name, then a slash. For example: traces/trace1

**Defaults** — None.

**Access** — Enabled.

**History** —Introduced in MSS Version 3.0.

**Examples** — To save trace data into the file trace1 in the subdirectory traces, type the following command:

WX4400# save trace traces/trace1

---

**set trace authentication**

Traces authentication information.

**Syntax** — set trace authentication [mac-addr mac-address] [port port-num] [user username] [level level]

- *mac-addr mac-address* — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- *port port-num* — Traces on a WX port number.
- *user username* — Traces a user. Specify a username of up to 32 alphanumeric characters with no spaces.
- *level level* — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

**Defaults** — The default trace level is 5.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.
**Examples** — The following command starts a trace for information about user jose’s authentication:

```
WX4400# set trace authentication user jose
success: change accepted.
```

**See Also**
- `clear trace` on page 740
- `display trace` on page 741
set trace dot1x  

Traces 802.1X sessions.

Syntax — set trace dot1x [mac-addr mac-address] [port port-num] [user username] [level level]

- **mac-addr mac-address** — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port port-num** — Traces on a WX port number.
- **user username** — Traces a user. Specify a username of up to 80 alphanumeric characters with no spaces.
- **level level** — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

Defaults — The default trace level is 5.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — The following command starts a trace for the 802.1X sessions for MAC address 00:01:02:03:04:05:

```
WX4400# set trace dot1x mac-addr 00:01:02:03:04:05: success: change accepted.
```

See Also

- **clear trace** on page 740
- **display trace** on page 741
set trace sm

Traces session manager activity.

**Syntax** — `set trace sm [mac-addr mac-address] [port port-num] [user username] [level level]`

- **mac-addr mac-address** — Traces a MAC address. Specify a MAC address, using colons to separate the octets (for example, 00:11:22:aa:bb:cc).
- **port port-num** — Traces on a WX port number.
- **user username** — Traces a user. Specify a username of up to 80 alphanumeric characters, with no spaces.
- **level level** — Determines the quantity of information included in the output. You can set the level with an integer from 1 to 10, where level 10 provides the most information. Levels 1 through 5 provide user-readable information. If you do not specify a level, level 5 is the default.

**Defaults** — The default trace level is 5.a

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — Type the following command to trace session manager activity for MAC address 00:01:02:03:04:05:

```
WX4400# set trace sm mac-addr 00:01:02:03:04:05: user username: level level: success: change accepted.
```

**See Also**

- `clear trace` on page 740
- `display trace` on page 741
SNOOP COMMANDS

Use snoop commands to monitor wireless traffic, by using a MAP as a sniffing device. The MAP copies the sniffed 802.11 packets and sends the copies to an observer, which is typically a protocol analyzer such as Ethereal or Tetherereal.

(For more information, including setup instructions for the monitoring station, see the “Remotely Monitoring Traffic” section in the “Troubleshooting a WX Switch” chapter of the Wireless LAN Switch and Controller Configuration Guide.)

This chapter presents snoop commands alphabetically. Use the following table to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Commands by Usage</th>
<th>Remote Monitoring (Snooping)</th>
<th>set snoop on page 749</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>display snoop info on page 754</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display snoop stats on page 756</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear snoop on page 748</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set snoop map on page 752</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display snoop map on page 755</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display snoop on page 754</td>
<td></td>
</tr>
<tr>
<td></td>
<td>clear snoop map on page 748</td>
<td></td>
</tr>
<tr>
<td></td>
<td>set snoop mode on page 753</td>
<td></td>
</tr>
<tr>
<td></td>
<td>display snoop stats on page 756</td>
<td></td>
</tr>
</tbody>
</table>
clear snoop

Deletes a snoop filter.

**Syntax** — `clear snoop filter-name`

- `filter-name` — Name of the snoop filter.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Examples** — The following command deletes snoop filter `snoop1`:

```
WX1200# clear snoop snoop1
```

**See Also**

- `set snoop` on page 749
- `display snoop info` on page 754

---

clear snoop map

Removes a snoop filter from a MAP radio.

**Syntax** — `clear snoop map filter-name ap ap-num radio {1 | 2}`

- `filter-name` — Name of the snoop filter.
- `ap ap-num` — Number of a MAP to which the snoop filter is mapped.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.
**Examples** — The following command removes snoop filter `snoop2` from radio 2 on Distributed MAP 3:

WX1200# clear snoop map snoop2 ap 3 radio 2
success: change accepted.

The following command removes all snoop filter mappings from all radios:

WX1200# clear snoop map all
success: change accepted.

**See Also**

- `display snoop` on page 754
- `display snoop map` on page 755
- `set snoop map` on page 752

---

**set snoop**

Configures a snoop filter.

**Syntax** — `set snoop filter-name [condition-list] [observer ip-addr] [snap-length num]`

- `filter-name` — Name for the filter. The name can be up to 32 alphanumeric characters, with no spaces.
- `condition-list` — Match criteria for packets. Conditions in the list are ANDed. Therefore, to be copied and sent to an observer, a packet must match all criteria in the `condition-list`. You can specify up to eight of the following conditions in a filter, in any order or combination:
  - `frame-type {eq | neq} {beacon | control | data | management | probe}`
  - `channel {eq | neq} channel`
  - `bssid {eq | neq} bssid`
  - `src-mac {eq | neq} mac-addr`
  - `dest-mac {eq | neq} mac-addr`
  - `host-mac {eq | neq} mac-addr`
  - `mac-pair mac-addr1 mac-addr2`
  - `direction {eq | neq} {transmit | receive}`
To match on packets to or from a specific MAC address, use the `dest-mac` or `src-mac` option. To match on both send and receive traffic for a host address, use the `host-mac` option. To match on a traffic flow (source and destination MAC addresses), use the `mac-pair` option. This option matches for either direction of a flow, and either MAC address can be the source or destination address.

If you omit a condition, all packets match that condition. For example, if you omit `frame-type`, all frame types match the filter.

For most conditions, you can use `eq` (equal) to match only on traffic that matches the condition value. Use `neq` (not equal) to match only on traffic that is not equal to the condition value.

- `observer ip-addr` — Specifies the IP address of the station where the protocol analyzer is located. If you do not specify an observer, the MAP radio still counts the packets that match the filter.

- `snap-length num` — Specifies the maximum number of bytes to capture. If you do not specify a length, the entire packet is copied and sent to the observer. 3Com recommends specifying a snap length of 100 bytes or less.

**Defaults** — No snoop filters are configured by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0. Version 6.0 added the direction filter.

**Usage** — Traffic that matches a snoop filter is copied after it is decrypted. The decrypted (clear) version is sent to the observer.

For best results:

- Do not specify an observer that is associated with the MAP where the snoop filter is running. This configuration causes an endless cycle of snoop traffic.

- If the snoop filter is running on a Distributed MAP, and the MAP used a DHCP server in its local subnet to configure its IP information, and the MAP did not receive a default gateway address as a result, the observer must also be in the same subnet. Without a default gateway, the MAP cannot find the observer.
The MAP that is running a snoop filter forwards snooped packets directly to the observer. This is a one-way communication, from the MAP to the observer. If the observer is not present, the MAP still sends the snoop packets, which use bandwidth. If the observer is present but is not listening to TZSP traffic, the observer continuously sends ICMP error indications back to the MAP. These ICMP messages can affect network and MAP performance.

**Examples** — The following command configures a snoop filter named `snoop1` that matches on all traffic, and copies the traffic to the device that has IP address 10.10.30.2:

```
WX1200# set snoop snoop1 observer 10.10.30.2 snap-length 100
```

The following command configures a snoop filter named `snoop2` that matches on all data traffic between the device with MAC address aa:bb:cc:dd:ee:ff and the device with MAC address 11:22:33:44:55:66, and copies the traffic to the device that has IP address 10.10.30.3:

```
```

**See Also**

- `clear snoop` on page 748
- `display snoop info` on page 754
- `display snoop stats` on page 756
- `set snoop map` on page 752
- `set snoop mode` on page 753
set snoop map

Maps a snoop filter to a radio on a MAP. A snoop filter does take effect until you map it to a radio and enable the filter.

Syntax — set snoop map filter-name ap ap-num radio {1 | 2}

- **filter-name** — Name of the snoop filter.
- **ap ap-num** — Number of a MAP to which to map the snoop filter.
- **radio 1** — Radio 1 of the MAP.
- **radio 2** — Radio 2 of the MAP. (This option does not apply to single-radio models.)

Defaults — Snoop filters are unmapped by default.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — You can map the same filter to more than one radio. You can map up to eight filters to the same radio. If more than one filter has the same observer, the MAP sends only one copy of a packet that matches a filter to the observer. After the first match, the MAP sends the packet and stops comparing the packet against other filters for the same observer.

If the filter does not have an observer, the MAP still maintains a counter of the number of packets that match the filter. (See *display snoop stats* on page 756.)

Examples — The following command maps snoop filter *snoop1* to radio 2 on MAP 3:

WX1200# set snoop map snoop1 ap 3 radio 2
success: change accepted.

See Also

- **clear snoop map** on page 748
- **display snoop map** on page 755
- **display snoop stats** on page 756
- **set snoop** on page 749
- **set snoop mode** on page 753
**set snoop mode**

Enables a snoop filter. A snoop filter does not take effect until you map it to a MAP radio and enable the filter.

**Syntax**

```
set snoop {filter-name | all}
mode {enable [stop-after num-pkts] | disable}
```

- `filter-name | all` — Name of the snoop filter. Specify `all` to enable all snoop filters.
- `enable` — Enables the snoop filter.
- `disable` — Disables the snoop filter.

**Defaults** — Snoop filters are disabled by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0. Version 6.0 removed the `stop-after` option. Also filter mode was made persistent across restarts.

**Usage** — The filter mode is retained even if you disable and reenable the radio, or restart the MAP or the WX switch. Once the filter is enabled, you must use the `disable` option to disable it.

**Examples** — The following command enables snoop filter `snoop1`:

```
WX# set snoop snoop1 mode enable
success: filter 'snoop1' enabled
```

**See Also**

- `display snoop` on page 754
- `display snoop info` on page 754
- `display snoop map` on page 755
- `display snoop stats` on page 756
display snoop

Displays the MAP radio mapping for all snoop filters.

Syntax — display snoop

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.

Usage — To display the mappings for a specific MAP radio, use the display snoop map command.

Examples — The following command shows the MAP radio mappings for all snoop filters configured on a WX switch:

```
WX1200# display snoop
ap: 3          Radio: 2
    snoop1
    snoop2
ap: 2          Radio: 2
    snoop2
```

See Also

- clear snoop map on page 748
- display snoop map on page 755
- set snoop map on page 752

display snoop info

Shows the configured snoop filters.

Syntax — display snoop filter-name

filter-name — Name of the snoop filter.

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 4.0.
**Examples** — The following command shows the snoop filters configured in the examples above:

WX1200# display snoop info
snoop1:
    observer 10.10.30.2 snap-length 100
    all packets
snoop2:
    observer 10.10.30.3 snap-length 100
    frame-type eq data

**See Also**
- clear snoop on page 748
- set snoop on page 749

---

**display snoop map** Shows the MAP radios that are mapped to a specific snoop filter.

**Syntax** — `display snoop map filter-name`

- **filter-name** — Name of the snoop filter.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — To display the mappings for all snoop filters, use the `display snoop` command.

**Examples** — The following command shows the mapping for snoop filter snoop1:

WX1200# display snoop map snoop1
filter 'snoop1' mapping
    ap: 3          Radio: 2

**See Also**
- clear snoop map on page 748
- display snoop on page 754
- set snoop map on page 752
display snoop stats  
Displays statistics for enabled snoop filters.

**Syntax** — `display snoop stats [filter-name [ap-num [radio {1 | 2}]]]

- `filter-name` — Name of the snoop filter.
- `ap-num` — Number of a Distributed MAP to which the snoop filter is mapped.
- `radio 1` — Radio 1 of the MAP.
- `radio 2` — Radio 2 of the MAP. (This option does not apply to single-radio models.)

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.0.

**Usage** — The MAP retains statistics for a snoop filter until the filter is changed or disabled. The MAP then clears the statistics.

**Examples** — The following command shows statistics for snoop filter `snoop1`:

```
WX1200# display snoop stats snoop1
Filter   ap Radio Rx Match Tx Match Dropped Stop-After
==============================================
snoop1    3     1 96 4 0 stopped
```
Table 119 describes the fields in this display.

**Table 119**  
display snoop stats Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter</td>
<td>Name of the snoop filter.</td>
</tr>
<tr>
<td>Dap</td>
<td>Distributed MAP containing the radio to which the filter is mapped.</td>
</tr>
<tr>
<td>Radio</td>
<td>Radio to which the filter is mapped.</td>
</tr>
<tr>
<td>Rx Match</td>
<td>Number of packets received by the radio that match the filter.</td>
</tr>
<tr>
<td>Tx Match</td>
<td>Number of packets sent by the radio that match the filter.</td>
</tr>
<tr>
<td>Dropped</td>
<td>Number of packets that matched the filter but that were not copied to the observer due to memory or network problems.</td>
</tr>
<tr>
<td>Stop-After</td>
<td>Filter state:</td>
</tr>
<tr>
<td></td>
<td>- running—enabled</td>
</tr>
<tr>
<td></td>
<td>- stopped—disabled</td>
</tr>
<tr>
<td></td>
<td>- number-of-packets—If the filter is running and the stop-after option was used to stop the filter, this field displays the number of packets that still need to match before the filter is stopped.</td>
</tr>
</tbody>
</table>
Use the system log commands to record information for monitoring and troubleshooting. MSS system logs are based on RFC 3164, which defines the log protocol.

This chapter presents system log commands alphabetically. Use Table 120 to locate commands in this chapter based on their use.

### Table 120  System Log Commands by Usage

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Logs</strong></td>
<td><strong>set log</strong> on page 764</td>
</tr>
<tr>
<td></td>
<td><strong>set log mark</strong> on page 767</td>
</tr>
<tr>
<td></td>
<td><strong>display log buffer</strong> on page 760</td>
</tr>
<tr>
<td></td>
<td><strong>display log config</strong> on page 762</td>
</tr>
<tr>
<td></td>
<td><strong>display log trace</strong> on page 763</td>
</tr>
<tr>
<td></td>
<td><strong>clear log</strong> on page 759</td>
</tr>
</tbody>
</table>

**clear log**

Clears the log messages stored in the log buffer, or removes the configuration for a syslog server and stops sending log messages to that server.

**Syntax** — `clear log [buffer | server ip-addr]`

- **buffer** — Deletes the log messages stored in nonvolatile storage.
- **server ip-addr** — Deletes the configuration for and stops sending log messages to the syslog server at this IP address. Specify an address in dotted decimal notation.

**Defaults** — None.
CHAPTER 23: SYSTEM LOG COMMANDS

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Examples** — To stop sending system logging messages to a server at 192.168.253.11, type the following command:

```
WX4400# clear log server 192.168.253.11
success: change accepted.
```

Type the following command to clear all messages from the log buffer:

```
WX4400# clear log buffer
success: change accepted.
```

**See Also**
- `clear log trace` on page 740
- `set log` on page 764

---

display log buffer

Displays system information stored in the nonvolatile log buffer or the trace buffer.

**Syntax** — `display log buffer [{+|-}number-of-messages] [facility facility-name] [matching string] [severity severity-level]`

- **buffer** — Displays the log messages in nonvolatile storage.
- **+|- number-of-messages** — Displays the number of messages specified as follows:
  - A positive number (for example, `+100`), displays that number of log entries starting from the oldest in the log.
  - A negative number (for example, `-100`) displays that number of log entries starting from newest in the log.
- **facility facility-name** — Area of MSS that is sending the log message. Type a space and a question mark (?) after display `log buffer facility` for a list of valid facilities.
- **matching string** — Displays messages that match a string—for example, a username or IP address.
- **severity severity-level** — Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:
  - **emergency** — The WX switch is unusable.
  - **alert** — Action must be taken immediately.
  - **critical** — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
  - **error** — The WX is missing data or is unable to form a connection.
  - **warning** — A possible problem exists.
  - **notice** — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
  - **info** — Informational messages only. No problem exists.
  - **debug** — Output from debugging.

**Defaults** — None.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0.

**Usage** — The debug level produces a lot of messages, many of which can appear to be somewhat cryptic. Debug messages are used primarily by 3Com for troubleshooting and are not intended for administrator use.

**Examples** — Type the following command to see the facilities for which you can view event messages archived in the buffer:

```
WX4400# display log buffer facility ?
<facility name> Select one of: KERNEL, AAA, SYSLOGD, ACL, APM, ARP, ASO, BOOT, CLI, CLUSTER, COPP, CRYPTO, DOT1X, NET, ETHERNET, GATEWAY, HTTPD, IGMP, IP, MISC, NOSE, NP, RAND, RESOLV, RIB, ROAM, ROGUE, SM, SNMPD, SPAN, STORE, SYS, TAGMGR, TBRIDGE, TCPSSL, TELNET, TFTP, TLS, TUNNEL, VLAN, X509, XML, MAP, RAPDA, WEBVIEW, EAP, FP, STAT, SSHD, SUP, DSNDS, CONFIG, BACKUP.
```

The following command displays logged messages for the AAA facility:

```
WX4400# display log buffer facility AAA
AAA Jun. 25 09:11:32.579848 ERROR AAA_NOTIFY_ERR: AAA got SM special event (98) on locality 3950 which is gone
```
See Also

- clear log on page 759
- display log config on page 762

display log config

Displays log configuration information.

Syntax — display log config

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — To display how logging is configured, type the following command:

WX4400# display log config
Logging console:        disabled
Logging console severity: DEBUG
Logging sessions:       disabled
Logging sessions severity: INFO
Logging buffer:         enabled
Logging buffer severity: DEBUG
Logging trace:          enabled
Logging trace severity: DEBUG
Logging buffer size:    10485760 bytes
Log marking:            disabled
Log marking severity:   NOTICE
Log marking interval    300 seconds

Logging server:        172.21.12.19 port514 severity EMERGENCY
Current session:       disabled
Current session severity: INFO

See Also

- clear log on page 759
- set log on page 764
**display log trace**

Displays system information stored in the nonvolatile log buffer or the trace buffer.

**Syntax**

```
display log trace [[+|-|/]number-of-messages] [facility facility-name] [matching string] [severity severity-level]
```

- **trace** — Displays the log messages in the trace buffer.
- **+|-|/number-of-messages** — Displays the number of messages specified as follows:
  - A positive number (for example, `+100`) displays that number of log entries starting from the oldest in the log.
  - A negative number (for example, `-100`) displays that number of log entries starting from newest in the log.
  - A number preceded by a slash (for example, `/100`) displays that number of the most recent log entries in the log, starting with the least recent.
- **facility facility-name** — Area of MSS that is sending the log message. Type a space and a question mark (?) after `display log trace facility` for a list of valid facilities.
- **matching string** — Displays messages that match a string—for example, a username or IP address.
- **severity severity-level** — Displays messages at a severity level greater than or equal to the level specified. Specify one of the following:
  - **emergency** — The WX switch is unusable.
  - **alert** — Action must be taken immediately.
  - **critical** — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
  - **error** — The WX is missing data or is unable to form a connection.
  - **warning** — A possible problem exists.
  - **notice** — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
  - **info** — Informational messages only. No problem exists.
  - **debug** — Output from debugging.
CHAPTER 23: SYSTEM LOG COMMANDS

Defaults — None.

Access — Enabled.

History — Introduced in MSS Version 3.0.

Examples — Type the following command to see the facilities for which you can view event messages archived in the buffer:

WX4400# display log trace facility ?

See Also
- display log config on page 762
- clear log on page 759

set log

Enables or disables logging of WX and MAP events to the WX log buffer or other logging destination and sets the level of the events logged. For logging to a syslog server only, you can also set the facility logged.

Syntax — set log {buffer | console | current | sessions | trace} [severity severity-level] enable | disable

set log server ip-addr [port port-number] severity severity-level [local-facility facility-level]

- buffer — Sets log parameters for the log buffer in nonvolatile storage.
- console — Sets log parameters for console sessions.
- current — Sets log parameters for the current Telnet or console session. These settings are not stored in nonvolatile memory.
- server ip-addr — Sets log parameters for a syslog server. Specify an address in dotted decimal notation.
- sessions — Sets the default log values for Telnet sessions. You can set defaults for the following log parameters:
  - Severity
• Logging state (enabled or disabled)

To override the session defaults for an individual session, type the `set log` command from within the session and use the `current` option.

• `trace` — Sets log parameters for trace files.

• `Port port-number` — Sets the TCP port for sending messages to the syslog server. You can specify a number from 1 to 65535. The default syslog port is 514.

• `severity severity-level` — Logs events at a severity level greater than or equal to the level specified. Specify one of the following:
  • `emergency` — The WX switch is unusable.
  • `alert` — Action must be taken immediately.
  • `critical` — You must resolve the critical conditions. If the conditions are not resolved, the WX can reboot or shut down.
  • `error` — The WX is missing data or is unable to form a connection.
  • `warning` — A possible problem exists.
  • `notice` — Events that potentially can cause system problems have occurred. These are logged for diagnostic purposes. No action is required.
  • `info` — Informational messages only. No problem exists.
  • `debug` — Output from debugging.

• `local-facility facility-level` — For messages sent to a syslog server, maps all messages of the severity you specify to one of the standard local log facilities defined in RFC 3164. You can specify one of the following values:
  • 0 — maps all messages to `local0`.
  • 1 — maps all messages to `local1`.
  • 2 — maps all messages to `local2`.
  • 3 — maps all messages to `local3`.
  • 4 — maps all messages to `local4`.
  • 5 — maps all messages to `local5`.
  • 6 — maps all messages to `local6`.
  • 7 — maps all messages to `local7`. 
If you do not specify a local facility, MSS sends the messages with their default MSS facilities. For example, AAA messages are sent with facility 4 and boot messages are sent with facility 20 by default.

- **enable** — Enables messages to the specified target.
- **disable** — Disables messages to the specified target.

**Defaults** — The following are defaults for the **set log** commands.

- Events at the error level and higher are logged to the WX console.
- Events at the error level and higher are logged to the WX system buffer.
- Trace logging is enabled, and debug-level output is stored in the WX trace buffer.

**Access** — Enabled.

**History** — Introduced in MSS Version 3.0. Version 4.2 added the option port.

**Usage** — Using the command with only **enable** or **disable** turns logging on or off for the target at all levels. For example, entering **set log buffer enable** with no other keywords turns on logging to the system buffer of all facilities at all levels. Entering **set log buffer disable** with no other keywords turns off all logging to the buffer.

**Examples** — To log only emergency, alert, and critical system events to the console, type the following command:

```
WX4400# set log console severity critical enable
success: change accepted.
```

**See Also**

- **display log config** on page 762
- **clear log** on page 759
**set log mark**

Configures MSS to generate mark messages at regular intervals. The mark messages indicate the current system time and date. 3Com can use the mark messages to determine the approximate time when a system restart or other event causing a system outage occurred.

**Syntax** — `set log mark [enable | disable] [severity level] [interval interval]`

- **enable** — Enables the mark messages.
- **disable** — Disables the mark messages.
- **severity level** — Log severity at which the messages are logged:
  - emergency
  - alert
  - critical
  - error
  - warning
  - notice
  - info
  - debug
- **interval interval** — Interval at which MSS generates the mark messages. You can specify from 1 to 2147483647 seconds.

**Defaults** — Mark messages are disabled by default. When they are enabled, MSS generates a message at the notice level once every 300 seconds by default.

**Access** — Enabled.

**History** — Introduced in MSS Version 4.1.

**Examples** — The following command enables mark messages:

```plaintext
WX1200# set log mark enable
success: change accepted.
```

**See Also**

- `display log config` on page 762
Boot prompt commands enable you to perform basic tasks, including booting a system image file, from the boot prompt (boot>). A CLI session enters the boot prompt if MSS does not boot successfully or you intentionally interrupt the boot process. To interrupt the boot process, press q followed by Enter (return).

**CAUTION:** Generally, boot prompt commands are used only for troubleshooting. 3Com recommends that you use these commands only when working with 3Com Technical Support to diagnose a system issue. In particular, commands that change boot parameters can interfere with a WX switch’s ability to boot successfully.

---

## Boot Prompt Commands by Usage

This chapter presents boot prompt commands alphabetically. Use Table 121 to locate commands in this chapter based on their use.

<table>
<thead>
<tr>
<th>Type</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Information</td>
<td><code>ls</code> on page 782</td>
</tr>
<tr>
<td></td>
<td><code>help</code> on page 781</td>
</tr>
<tr>
<td>Booting</td>
<td><code>boot</code> on page 771</td>
</tr>
<tr>
<td></td>
<td><code>reset</code> on page 784</td>
</tr>
<tr>
<td></td>
<td><code>autoboot</code> on page 770</td>
</tr>
<tr>
<td></td>
<td><code>dhcp</code> on page 776</td>
</tr>
<tr>
<td>File Management</td>
<td><code>dir</code> on page 777</td>
</tr>
<tr>
<td></td>
<td><code>fver</code> on page 780</td>
</tr>
<tr>
<td></td>
<td><code>version</code> on page 786</td>
</tr>
</tbody>
</table>
**autoboot**

Displays or changes the state of the autoboot option. The autoboot option controls whether a WX switch automatically boots a system image after initializing the hardware, following a system reset or power cycle.

**Syntax** — `autoboot [ON | on | OFF | off]`

- **ON** — Enables the autoboot option.
- **on** — Same effect as **ON**.
- **OFF** — Disables the autoboot option.
- **off** — Same effect as **OFF**.

**Defaults** — The autoboot option is enabled by default.

**Access** — Boot prompt.

**History** —Introduced in MSS Version 3.0.

**Examples** — The following command displays the current setting of the autoboot option:

```
boot> autoboot
The autoboot flag is on.
```

**See Also**

- **boot** on page 771
**boot**

Loads and executes a system image file.

**Syntax** — `boot [BT=type] [DEV=device] [FN=filename] [HA=ip-addr] [FL=num] [OPT=option] [OPT+=option]`

- **BT=type** — Boot type:
  - c — Compact flash. Boots using nonvolatile storage or a flash card.
  - n — Network. Boots using a TFTP server.
- **DEV=device** — Location of the system image file:
  - c: — Nonvolatile storage area containing boot partition 0
  - d: — Nonvolatile storage area containing boot partition 1
  - e: — Primary partition of the flash card in the flash card slot
  - f: — Secondary partition of the flash card in the flash card slot
  - boot0 — boot partition 0
  - boot1 — boot partition 1
- **FN=filename** — System image filename.
- **HA=ip-addr** — Host address (IP address) of a TFTP server. This parameter applies only when the boot type is `n` (network).
- **FL=num** — Number representing the bit settings of boot flags to pass to the booted system image. Use this parameter only if advised to do so by 3Com.
- **OPT=option** — String up to 128 bytes of boot options to pass to the booted system image *instead of* the boot option(s) in the currently active boot profile. The options temporarily replace the options in the boot profile. Use this parameter only if advised to do so by 3Com.
- **OPT+=option** — String up to 128 bytes of boot options to pass to the booted system image *in addition to* the boot option(s) in the currently active boot profile. The options are appended to the options already in the boot profile. Use this parameter only if advised to do so by 3Com.

**Defaults** — The boot settings in the currently active boot profile are used by default.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 3.0.
**Usage** — If you use an optional parameter, the parameter setting overrides the setting of the same parameter in the currently active boot profile. However, the boot profile itself is not changed. To display the currently active boot profile, use the **display** command. To change the currently active boot profile, use the **change** command.

**Examples** — The following command loads system image file WXA30001.Rel from boot partition 1:

```
boot> boot PN=WXA03001.Rel DEV=boot1
Compact Flash load from boot0:WXA03001.Rel.
unzip: Inflating ramdisk_3.0.1_092304_WX4400 OK
unzip file len 36196930 OK
```

Detecting hardware...done.
readclock: 2004-9-29 21:45:7.31 UTC
system initialized (3.0.1), starting MSS
Executing update_3
Starting supervisor 3.0.1_092304_WX4400 ...

SNMPD Sep 29 21:45:34.262293 NOTICE SNMPD: SNMP Agent Resident Module Version 16.1.0.0
SNMPD Sep 29 21:45:34.263146 NOTICE SNMPD: Copyright (c) 2004 3Com Corporation. All rights reserved.
SYS Sep 29 21:45:36.849457 NOTICE Port 1 up 1000 Full Duplex
SYSLOGD Sep 29 21:45:38.857125 ALERT SYSTEM_READY: The system has finished booting. (cause was "Warm Reboot")

Copyright (c) 2004 3Com Corporation. All rights reserved.

Username:

**See Also**

- **change** on page 773
- **display** on page 778
change

Changes parameters in the currently active boot profile. (For information about boot profiles, see display on page 778.)

Syntax — change

Defaults — The default boot type is c (compact flash). The default filename is default. The default flags setting is 0x00000000 (all flags disabled) and the default options list is run=nos;boot=0. The default device setting is the boot partition specified by the most recent set boot partition command typed at the Enabled level of the CLI, or boot 0 if the command has never been typed.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — After you type the change command, the system interactively displays the current setting of each parameter and prompts you for the new setting. When prompted, type the new setting, press Enter to accept the current setting, or type . (period) to change the setting to its default value. To back up to the previous parameter, type - (hyphen).

For information about each of the boot parameters you can set, see display on page 778.

Examples — The following command enters the configuration mode for the currently active boot profile, changes the device to boot1, and leaves the other parameters with their current settings:

    boot> change
    Changing the default configuration is not recommended.
    Are you sure that you want to proceed? (y/n)

    BOOT TYPE: [c]
    DEVICE: [boot0:]boot1
    FILENAME: [default]
    FLAGS: [0x00000000]
    OPTIONS: [run=nos;boot=0]
The following command enters the configuration mode for the currently active boot profile and configures the WX switch (in this example, an WXR100) to boot using a TFTP server:

```
boot> change
Changing the default configuration is not recommended.
Are you sure that you want to proceed? (y/n)y
```

BOOT TYPE: [c] > n
DEVICE: [boot0: ] > emac1
FILENAME: [default] > bootfile
HOST IP: [0.0.0.0] > 172.16.0.1
LOCAL IP: [0.0.0.0] > 172.16.0.21
GATEWAY IP: [0.0.0.0] > 172.16.0.20
IP MASK: [0.0.0.0] > 255.255.255.0
FLAGS: [0x00000000]
OPTIONS: [run=nos; boot=0]

See Also

- `boot` on page 771
- `create` on page 774
- `delete` on page 775
- `dhcp` on page 776
- `display` on page 778
- `next` on page 783

---

### create

Creates a new boot profile. (For information about boot profiles, see `display` on page 778.)

**Syntax** — create

**Defaults** — The new boot profile has the same settings as the currently active boot profile by default.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 3.0.
**Usage** — A WX switch can have up to four boot profiles. The boot profiles are stored in slots, numbered 0 through 3. When you create a new profile, the system uses the next available slot for the profile. If all four slots already contain profiles and you try to create a fifth profile, the switch displays a message advising you to change one of the existing profiles instead.

To make a new boot profile the currently active boot profile, use the **next** command. To change boot parameter settings, use the **change** command.

**Examples** — The following command creates a new boot profile in slot 1 on a WX switch that currently has only one boot profile, in slot 0:

```
boot> create

BOOT Index:   1
BOOT TYPE:    c
DEVICE:       boot1:
FILENAME:     default
FLAGS:        00000000
OPTIONS:      run=nos;boot=0
```

**See Also**
- **change** on page 773
- **delete** on page 775
- **display** on page 778
- **next** on page 783

---

**delete**

Removes the currently active boot profile. (For information about boot profiles, see **display** on page 778.)

**Syntax** — **delete**

**Defaults** — None.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 3.0.
**Usage** — When you type the `delete` command, the next-lower numbered boot profile becomes the active profile. For example, if the currently active profile is number 3, profile number 2 becomes active after you type `delete` to delete profile 3. You cannot delete boot profile 0.

**Examples** — To remove the currently active boot profile, type the following command:

```
boot> delete
```

```
BOOT Index:   1
BOOT TYPE:    c
DEVICE:       boot1:
FILENAME:     default
FLAGS:        00000000
OPTIONS:      run=nos;boot=0
```

**See Also**
- `change` on page 773
- `create` on page 774
- `display` on page 778
- `next` on page 783

---

**dhcp**

Displays or changes the state of the DHCP option. The DHCP option controls whether a WX switch uses DHCP to obtain its IP address when it is booted using a TFTP server.

**Syntax** — `dhcp [ON | on | OFF | off]`

- **ON** — Enables the DHCP option.
- **on** — Same effect as **ON**.
- **OFF** — Disables the DHCP option.
- **off** — Same effect as **OFF**.

**Defaults** — The DHCP option is disabled by default.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 1.0.
Examples — The following command displays the current setting of the DHCP option:

```
boot> dhcp
DHCP is currently enabled.
```

The following command disables the DHCP option:

```
boot> dhcp
DHCP is currently disabled.
```

See Also

- `boot` on page 771

---

diag

Accesses the diagnostic mode.

Syntax — `diag`

Defaults — The diagnostic mode is disabled by default.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — Access to the diagnostic mode requires a password, which is not user configurable. Use this mode only if advised to do so by 3Com.

---

dir

Displays the boot code and system image files on a WX switch.

Syntax — `dir [c: | d: | e: | f: | boot0 | boot1]`

- `c:` — Nonvolatile storage area containing boot partition 0 (primary).
- `d:` — Nonvolatile storage area containing boot partition 1 (secondary).
- `e:` — Primary partition of the flash card in the flash card slot.
- `f:` — Secondary partition of the flash card in the flash card slot.
- `boot0` — Boot partition 0.
- `boot1` — Boot partition 1.

Defaults — None.
Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — To display the system image software versions, use the `fver` command. This command does not list the boot code versions. To display the boot code versions, use the `version` command.

Examples — The following command displays all the boot code and system image files on a WX switch:

```plaintext
boot> dir

Internal Compact Flash Directory (Primary):
  WXA30001.Rel  8863722 bytes

Internal Compact Flash Directory (Secondary):
  WXA30001.Rel  8862885 bytes
```

See Also
- `fver` on page 780
- `version` on page 786

display

Displays the currently active boot profile. A boot profile is a set of parameters that a WX switch uses to control the boot process. Each boot profile contains the following parameters:

- **Boot type** — Either compact flash (local device on the WX switch) or network (TFTP)
- **Boot device** — Location of the system image file
- **Filename** — System image file
- **Flags** — Number representing the bit settings of boot flags to pass to the booted system image.
- **Options** — String up to 128 bytes of boot options to pass to the booted system image
A WX switch can have up to four boot profiles, numbered 0 through 3. Only one boot profile can be active at a time. You can create, change, and delete boot profiles. You also can activate another boot profile in place of the currently active one.

**Syntax** — `display`

**Defaults** — None.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 3.0.

**Examples** — To display the currently active boot profile, type the following command at the boot prompt:

```
boot> display
```

```
BOOT Index: 0
BOOT TYPE: c
DEVICE: boot1:
FILENAME: default
FLAGS: 00000000
OPTIONS: run=nos;boot=0
```

Table 122 describes the fields in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT Index</td>
<td>Boot profile slot, which can be a number from 0 to 3.</td>
</tr>
<tr>
<td>BOOT TYPE</td>
<td>Boot type:</td>
</tr>
<tr>
<td></td>
<td>- c — Compact flash. Boots using nonvolatile storage or a flash card.</td>
</tr>
<tr>
<td></td>
<td>- n — Network. Boots using a TFTP server.</td>
</tr>
</tbody>
</table>

Table 122  Output of display command
### fver
Displays the version of a system image file installed in a specific location on a WX switch.

**Syntax**

```plaintext
fver {c: | d: | e: | f: | boot0: | boot1:} [filename]
```

- `c:` — Nonvolatile storage area containing boot partition 0 (primary).
- `d:` — Nonvolatile storage area containing boot partition 1 (secondary).
- `e:` — Primary partition of the flash card in the flash card slot.
- `f:` — Secondary partition of the flash card in the flash card slot.
- `boot0:` — Boot partition 0.
- `boot1:` — Boot partition 1.
- `filename` — System image filename.

**Defaults** — None.
Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — To display the image filenames, use the dir command. This command does not list the boot code versions. To display the boot code versions, use the version command.

Examples — The following command displays the system image version installed in boot partition 1:

```
boot> fver boot1
File boot1:default version is 3.0.1.
```

See Also
- dir on page 777
- version on page 786

---

**help**

Displays a list of all the boot prompt commands or detailed information for an individual command.

Syntax — `help [command-name]`

- `command-name` — Boot prompt command.

Defaults — None.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.

Usage — If you specify a command name, detailed information is displayed for that command. If you do not specify a command name, all the boot prompt commands are listed.
**Examples** — The following command displays detailed information for the `fver` command:

```
boot> help fver
```

`fver` Display the version of the specified device:filename.

**USAGE:**  `fver [c:file|d:file|e:file|f:file|boot0:file|boot1:file|
boot2:file|boot3:file]`

Command to display the version of the compressed image file associated with the given device:filename.

**See Also**
- `ls` on page 782

---

**ls**

Displays a list of the boot prompt commands.

**Syntax** — `ls`

**Defaults** — None.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 3.0.

**Usage** — To display help for an individual command, type help followed by the command name (for example, `help boot`).
**Examples** — To display a list of the commands available at the boot prompt, type the following command:

```
boot> ls

ls     Display a list of all commands and descriptions.
help   Display help information for each command.
autoboot Display the state of, enable, or disable the autoboot option.
boot   Load and execute an image using the current boot configuration profile.
change Change the current boot configuration profile.
create Create a new boot configuration profile.
delete Delete the current boot configuration profile.
next   Select the next boot configuration profile.
display Display the current boot configuration profile.
dir    Display the contents of the specified boot partition.
fver   Display the version of the loadable image specified by device:filename.
version Display HW and Bootstrap/Bootloader version information.
reset  Reset the system.
test   Display the state of, enable, or disable the tests option.
diag   Access the diagnostic command CLI.
```

**See Also**
- help on page 781

**next**

Activates and displays the boot profile in the next boot profile slot. (For information about boot profiles, see `display` on page 778.)

**Syntax** — `next`

**Defaults** — None.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 3.0.

**Usage** — A WX switch contains 4 boot profile slots, numbered 0 through 3. This command activates the boot profile in the next slot, in ascending numerical order. If the currently active slot is 3, the command activates the boot profile in slot 0.
Examples — To activate the boot profile in the next slot and display the profile, type the following command:

```bash
boot> next
```

```
BOOT Index: 0
BOOT TYPE: c
DEVICE: boot1:
FILENAME: testcfg
FLAGS: 00000000
OPTIONS: run=nos;boot=0
```

See Also

- **change** on page 773
- **create** on page 774
- **delete** on page 775
- **display** on page 778

---

**reset**

Resets a WX switch’s hardware.

**Syntax** — `reset`

**Defaults** — None.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 3.0.

**Usage** — After resetting the hardware, the `reset` command attempts to load a system image file only if other boot settings are configured to do so.

Examples — To immediately reset the system, type the following command at the boot prompt:

```bash
boot> reset
```

```
WX Bootstrap 3.1 Release
Testing Low Memory 1 ............
Testing Low Memory 2 ............
CISTPL_VERS_1:  4.1   <SanDisk> <SDP> <5/3 0.6>
Reset Cause (0x0100) is WARM
```
3Com WX-4400 Bootstrap/Bootloader

Version 3.0.2 Release
Compiled on Wed Sep 22 09:18:47 PDT 2004 by

Bootstrap 0 version: 3.1 Active
Bootloader 0 version: 3.0.2 Active
Bootstrap 1 version: 3.1
Bootloader 1 version: 3.0.1

WX-4400 Board Revision: 2.
WX-4400 Controller Revision: 5.
WXA30001.Rel 8863722 bytes

BOOT Index: 0
BOOT TYPE: c
DEVICE: boot0:
FILENAME: default
FLAGS: 00000000
OPTIONS: run=nos;root=md0a

See Also
- boot on page 771

test

Displays or changes the state of the poweron test flag. The poweron test flag controls whether a WX performs a set of self tests prior to the boot process.

Syntax — test [ON | on | OFF | off]

- ON — Enables the poweron test flag.
- on — Same effect as ON.
- OFF — Disables the poweron test flag.
- off — Same effect as OFF.

Defaults — The poweron test flag is disabled by default.

Access — Boot prompt.

History — Introduced in MSS Version 3.0.
**Examples** — The following command displays the current setting of the poweron test flag:

```
boot> test
The diagnostic execution flag is not set.
```

**See Also**
- `boot` on page 771

---

**version**

Displays version information for a WX switch’s hardware and boot code.

**Syntax** — `version`

**Defaults** — None.

**Access** — Boot prompt.

**History** — Introduced in MSS Version 3.0.

**Usage** — This command does not list the system image file versions installed in the boot partitions. To display system image file versions, use the `dir` or `fver` command.

**Examples** — To display hardware and boot code version information, type the following command at the boot prompt:

```
boot> version
```

3Com WX-4400 Bootstrap/Bootloader

```
Version 3.0.2 Release
Compiled on Wed Sep 22 09:18:47 PDT 2004 by

Bootstrap 0 version: 3.1 Active
Bootloader 0 version: 3.0.2 Active
Bootstrap 1 version: 3.1
Bootloader 1 version: 3.0.1

WX-4400 Board Revision: 2.
WX-4400 Controller Revision: 5.
```

**See Also**
- `dir` on page 777
- `fver` on page 780
3Com offers product registration, case management, and repair services through eSupport.3com.com. You must have a user name and password to access these services, which are described in this appendix.

<table>
<thead>
<tr>
<th>Register Your Product to Gain Service Benefits</th>
<th>To take advantage of warranty and other service benefits, you must first register your product at:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="http://eSupport.3com.com/">http://eSupport.3com.com/</a></td>
</tr>
<tr>
<td></td>
<td>3Com eSupport services are based on accounts that are created or that you are authorized to access.</td>
</tr>
</tbody>
</table>

| Solve Problems Online                           | 3Com offers the following support tool: |
|                                                | ■ 3Com Knowledgebase — Helps you to troubleshoot 3Com products. This query-based interactive tool is located at: |
|                                                | http://knowledgebase.3com.com |
|                                                | It contains thousands of technical solutions written by 3Com support engineers. |
**Purchase Extended Warranty and Professional Services**

To enhance response times or extend your warranty benefits, you can purchase value-added services such as 24x7 telephone technical support, software upgrades, onsite assistance, or advanced hardware replacement.

Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. For more information on 3Com Extended Warranty and Professional Services, see:

http://www.3com.com/

Contact your authorized 3Com reseller or 3Com for additional product and support information. See the table of access numbers later in this appendix.

**Access Software Downloads**

You are entitled to *bug fix / maintenance releases* for the version of software that you initially purchased with your 3Com product. To obtain access to this software, you need to register your product and then use the Serial Number as your login. Restricted Software is available at:

http://eSupport.3com.com/

To obtain software releases that *follow* the software version that you originally purchased, 3Com recommends that you buy an Express or Guardian contract, a Software Upgrades contract, or an equivalent support contract from 3Com or your reseller. Support contracts that include software upgrades cover feature enhancements, incremental functionality, and bug fixes, but they do not include software that is released by 3Com as a separately ordered product. Separately orderable software releases and licenses are listed in the 3Com Price List and are available for purchase from your 3Com reseller.

**Contact Us**

3Com offers telephone, internet, and e-mail access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL, or e-mail address from the table in the next section.
To obtain telephone support as part of your warranty and other service benefits, you must first register your product at:

http://eSupport.3com.com/

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return materials authorization number (RMA). Products sent to 3Com without authorization numbers clearly marked on the outside of the package will be returned to the sender unopened, at the sender’s expense. If your product is registered and under warranty, you can obtain an RMA number online at http://eSupport.3com.com/. First-time users must apply for a user name and password.

Telephone numbers are correct at the time of publication. Find a current directory of 3Com resources by region at:

http://csoweb4.3com.com/contactus/

<table>
<thead>
<tr>
<th>Country</th>
<th>Telephone Number</th>
<th>Country</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>1800 075 316</td>
<td>Philippines</td>
<td>1800 144 10220 or</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>2907 0456</td>
<td>PR of China</td>
<td>029003078</td>
</tr>
<tr>
<td>India</td>
<td>000 800 440 1193</td>
<td>Singapore</td>
<td>800 810 0504</td>
</tr>
<tr>
<td>Indonesia</td>
<td>001 803 852 9825</td>
<td>South. Korea</td>
<td>800 616 1463</td>
</tr>
<tr>
<td>Japan</td>
<td>03 3507 5984</td>
<td>Taiwan</td>
<td>00801 444 318</td>
</tr>
<tr>
<td>Malaysia</td>
<td>1800 812 612</td>
<td>Thailand</td>
<td>001 800 441 2152</td>
</tr>
<tr>
<td>New Zealand</td>
<td>0800 450 454</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX A: OBTAINING SUPPORT FOR YOUR 3COM PRODUCTS

Pakistan Call the U.S. direct by dialing 00 800 01001, then dialing 800 763 6780
Sri Lanka Call the U.S. direct by dialing 02 430 430, then dialing 800 763 6780
Vietnam Call the U.S. direct by dialing 1 201 0288, then dialing 800 763 6780

You can also obtain non-urgent support in this region at this email address apr_technical_support@3com.com
Or request a return material authorization number (RMA) by FAX using this number: +61 2 9937 5048, or send an email at this email address: ap_rma_request@3com.com

Europe, Middle East, and Africa — Telephone Technical Support and Repair

From anywhere in these regions not listed below, call: +44 1442 435529

From the following countries, call the appropriate number:

<table>
<thead>
<tr>
<th>Country</th>
<th>Telephone Number</th>
<th>Country</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>0800 297 468</td>
<td>Luxembourg</td>
<td>800 23625</td>
</tr>
<tr>
<td>Belgium</td>
<td>0800 71429</td>
<td>Netherlands</td>
<td>0800 0227788</td>
</tr>
<tr>
<td>Denmark</td>
<td>800 17309</td>
<td>Norway</td>
<td>800 11376</td>
</tr>
<tr>
<td>Finland</td>
<td>0800 113153</td>
<td>Poland</td>
<td>00800 4411 357</td>
</tr>
<tr>
<td>France</td>
<td>0800 917959</td>
<td>Portugal</td>
<td>800 831416</td>
</tr>
<tr>
<td>Germany</td>
<td>0800 182 1502</td>
<td>South Africa</td>
<td>0800 995 014</td>
</tr>
<tr>
<td>Hungary</td>
<td>06800 12813</td>
<td>Spain</td>
<td>900 938 919</td>
</tr>
<tr>
<td>Ireland</td>
<td>1 800 553 117</td>
<td>Sweden</td>
<td>020 795 482</td>
</tr>
<tr>
<td>Israel</td>
<td>180 945 3794</td>
<td>Switzerland</td>
<td>0800 553 072</td>
</tr>
<tr>
<td>Italy</td>
<td>800 879489</td>
<td>U.K.</td>
<td>0800 096 3266</td>
</tr>
</tbody>
</table>

You can also obtain support in this region using this URL: http://emea.3com.com/support/email.html
You can also obtain non-urgent support in this region at these email addresses:
Technical support and general requests: customer_support@3com.com
Return material authorization: warranty_repair@3com.com
Contract requests: emea_contract@3com.com

Latin America — Telephone Technical Support and Repair

Antigua          | 1 800 988 2112 |
Argentina        | 0 810 444 3COM  |
Aruba            | 1 800 998 2112 |
Bahamas          | 1 800 998 2112 |
Barbados          | 1 800 998 2112 |
Belize           | 52 5 201 0010  |
Bermuda          | 1 800 998 2112 |
Bonaire          | 1 800 998 2112 |
Brazil           | 0800 13 3COM    |
Cayman           | 1 800 998 2112 |
Chile            | AT&T +800 998 2112 |
Colombia         | AT&T +800 998 2112 |
Costa Rica       | AT&T +800 998 2112 |
Curacao          | 1 800 998 2112 |
Ecuador          | AT&T +800 998 2112 |
Dominican Republic | AT&T +800 998 2112 |

You can also obtain support in this region in the following ways:

- Spanish speakers, enter the URL: http://lat.3com.com/lat/support/form.html
- Portuguese speakers, enter the URL: http://lat.3com.com/br/support/form.html
- English speakers in Latin America, send e-mail to: lat_support_anc@3com.com
<table>
<thead>
<tr>
<th>Country</th>
<th>Telephone Number</th>
<th>Country</th>
<th>Telephone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>US and Canada — Telephone Technical Support and Repair</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All locations:</td>
<td>Network Jacks; Wired or Wireless Network Interface Cards:</td>
<td>1 847-262-0070</td>
<td>1 800 876 3266</td>
</tr>
<tr>
<td>All other 3Com products:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
INDEX

A
autoboot 770

B
backup 712
boot 771

C
change 773
clear accounting 261
clear ap 118
clear ap boot-configuration 358
clear ap local-switching vlan-profile 355
clear ap radio 356
clear authentication admin 262
clear authentication console 263
clear authentication dot1x 264
clear authentication mac 265
clear authentication proxy 266
clear banner motd 90
clear boot backup-configuration 714
clear boot config 714
clear dot1x bonded-period 642
clear dot1x max-req 643
clear dot1x port-control 643
clear dot1x quiet-period 644
clear dot1x reauth-max 645
clear dot1x reauth-period 645
clear dot1x timeout auth-server 646
clear dot1x timeout supplicant 646
clear dot1x tx-period 647
clear fdb 152
clear history 91
clear igmp statistics 562
clear interface 185
clear ip alias 186
clear ip dns domain 187
clear ip dns server 187
clear ip route 188
clear ip telnet 189
clear location policy 267

clear log 759
clear log buffer 759
clear log server 759
clear log trace 740
clear mac-user 268
clear mac-user attr 269
clear mac-user group 269
clear mac-usergroup 270
clear mac-usergroup attr 271
clear mobility-domain 328
clear mobility-domain member 328
clear mobility-profile 272
clear network-domain 340
clear network-domain mode 341
clear network-domain peer 342
clear network-domain seed-ip 343
clear ntp server 189
clear ntp update-interval 190
clear port counters 119
clear port media-type 120
clear port mirror 121
clear port name 120
clear port type 122
clear port-group 119
clear qos 177
clear qos-profile 42
clear radio-profile 360
clear radius 626
clear radius client system-ip 627
clear radius das-port 35
clear radius server 629
clear rfdetect attack-list 678
clear rfdetect black-list 679
clear rfdetect ignore 679
clear rfdetect ssid-list 680
clear rfdetect vendor-list 681
clear security acl 586
clear security acl map 587
clear security L2-restrict 153
clear security L2-restrict counters 154
clear server group 629
clear server group load-balance 629
clear service-profile 361
clear sessions 661
clear sessions network 61, 663
clear snmp community 191
clear snmp notify profile 191
clear snmp notify target 192
clear snoop 748
clear snoop map 748
clear spantree portcost 532
clear spantree portpri 533
clear spantree portvlancost 533
clear spantree portvlanpri 534
clear spantree statistics 535
clear summertime 193
clear system 92
clear system countrycode 92
clear system ip-address 92, 194
clear system location 92
clear system name 92
clear timezone 194
clear trace 740
clear user 272
clear user attr 273
clear user group 274
clear user lockout 274
clear usergroup 275
clear usergroup attr 276
clear vlan 155
clear vlan-profile 156
commit security acl 589
copy 715
create 774
crypto certificate 612
crypto certificate admin 612
crypto certificate eap 612
crypto generate key 613
crypto generate request 614
crypto generate request admin 614
crypto generate request eap 614
crypto generate self-signed 616
crypto generate self-signed admin 616
crypto generate self-signed eap 616
crypto otp 618
crypto otp admin 618
crypto otp eap 618
crypto pkcs12 620
crypto pkcs12 admin 620
crypto pkcs12 eap 620
disable 85
display 778
display aaa 277
display accounting statistics 280
display ap boot-configuration 390
display ap config 54, 55, 362, 364, 529
display ap config radio 55
display ap config verbose 54
display ap connection 391
display ap counters 367
display ap etherstats 375
display ap fdb 373
display ap global 393
display ap group 377
display ap mesh-links 377
display ap qos-stats 374
display ap status 379
display ap unconfigured 395
display ap vlan 385
display arp 195
display auto-tune attributes 386
display auto-tune neighbors 388
display banner motd 93
display base-information 93
display boot 722
display config 723
display crypto ca-certificate 621
display crypto certificate 622
display crypto key domain 624
display crypto key ssh 624
display dhcp-client 196
display dhcp-server 198
display dot1x 647
display fdb 157
display fdb agingtime 159
display fdb count 160
display igmp 562
display igmp mrouter 566
display igmp querier 567
display igmp receiver-table 569
display igmp statistics 571
display interface 200
display ip alias 201
display ip dns 202
display ip https 203
display ip route 204
display ip telnet 206
display license 94
display load 95
display load cpu 57
display load cpu history 58
display load memory 56
display load-balancing group 396
display location policy 282
display log buffer 760
display log config 762
display log trace 763
display mac-user 51
display mac-usergroup 53
display mobility-domain config 329, 330
display mobility-domain status 331
display mobility-profile 283
display network-domain 344
display port counters 123
display port media-type 129
display port mirror 125
display port poe 126
display port status 127
display port-group 124
display qos 181
display qos dscp-table 182
display radio-profile 59, 398
display radius 48
display rfdetect attack-list 683
display rfdetect black-list 684
display rfdetect clients 685
display rfdetect countermeasures 687
display rfdetect counters 688
display rfdetect data 66, 690
display rfdetect data ap 69
display rfdetect data clients 70
display rfdetect data summary 72
display rfdetect data verbose 70
display rfdetect ignore 692
display rfdetect mobility-domain 692
display rfdetect ssid-list 697
display rfdetect vendor-list 697
display rfdetect visible 698
display roaming station 161
display roaming vlan 163
display security acl 590
display security acl editbuffer 590, 591
display security acl hits 592
display security acl info 593
display security acl map 594
display security acl resource-usage 595
display security L2-restrict 164
display service-profile 61, 401
display sessions 664, 667
display sessions mesh-ap 667
display sessions network 668
display sessions network ap 60
display sessions network ap radio 60
display sessions network apmap 60
display sessions network portal 60
display snmp community 209
display snmp counters 210

display snmp notify profile 210
display snmp notify target 210
display snmp status 211
display snmp usm 212
display snoop 754
display snoop info 754
display snoop map 755
display snoop stats 756
display span-tree 536
display span-tree backbonefast 539
display span-tree blockedports 540
display span-tree portfast 541
display span-tree portvlan cost 542
display span-tree statistics 542
display span-tree uplinkfast 548
display summertime 212
display system 95
display timedate 213
display timezone 213
display trace 741
display tunnel 165
display user 49
display usergroup 52
display version 725
display vlan config 166

E
et 706

F
fver 780

H
help 98, 781
history 99

I
install soda agent 721

L
load config 727
ls 782

M
md5 729
mkdir 729
monitor port counters 130
INDEX

N
next 783

P
ping 214

Q
quickstart 100
quit 86

R
radping 39
reset 784
reset ap 410
reset port 135
reset system 731
restore 732
rfdetect 47
rfping 682
rmdir 733
rollback security acl 599

S
save config 733
save trace 742
set accounting {admin | console} 283
set accounting {dot1x | mac | web | last-resort} 285
set ap 135
set ap auto 410
set ap auto mode 414
set ap auto persistent 412
set ap auto radiotype 413
set ap bias 415
set ap blink 416, 427
set ap boot-configuration mesh mode 418
set ap boot-configuration mesh psk-phrase 419
set ap boot-configuration mesh psk-raw 420
set ap boot-configuration mesh ssid 421
set ap boot-ip 417
set ap boot-switch 422
set ap boot-vlan 423
set ap fingerprint 424
set ap force-image-download 426
set ap local-switching mode 427
set ap local-switching mode vlan-profile 428
set ap name 429
set ap power-mode 31
set ap radio antenna-location 430
set ap radio antennatype 431
set ap radio auto-tune max-power 432
set ap radio auto-tune max-retransmissions 433
set ap radio channel 435
set ap radio link-calibration 436
set ap radio load balancing 437
set ap radio load balancing group 438
set ap radio mode 439
set ap radio radio-profile 440
set ap radio tx-power 441
set ap security 443
set ap upgrade-firmware 444, 446
set arp 216
set ap agingtime 217
set authentication admin 287
set authentication console 289
set authentication dot1x 291
set authentication mac 295
set authentication mac-prefix 36
set authentication max-attempts 297, 298
set authentication minimum-password-length 299
set authentication password-restrict 300
set authentication proxy 301
set authentication web 302
set authorization dynamic 35
set auto-config 100
set band-preference 445
set banner acknowledge 102
set banner motd 104
set boot backup-configuration 734
set boot backup-configuration 734
set boot configuration-file 735, 736
set cluster mode 30
set cluster preempt 30
set confirm 105
set domain security 337
set dot1x authcontrol 650
set dot1x bonded-period 651
set dot1x key-tx 652
set dot1x max-req 653
set dot1x port-control 654
set dot1x quiet-period 655
set dot1x reauth 655
set dot1x reauth-max 656
set dot1x reauth-period 657
set dot1x timeout auth-server 657
set dot1x timeout supplicant 658
set dot1x tx-period 658
set dot1x wep-rekey 659
set dot1x wep-rekey-period 660
set enablepass 87
set fdb 169
set fdb agingtime 170
set igmp 573
set igmp mrouter 575
set igmp mrsol 576
set igmp mrsol mrsi 576
set igmp qci 577
set igmp proxy-report 578
set igmp qi 579
set igmp qri 580
set igmp querier 581
set igmp receiver 581
set igmp rv 582
set interface 218
set interface dhcp-server 220
set interface status 221
set ip alias 222
set ip dns 223
set ip dns domain 223
set ip dns server 224
set ip https server 225
set ip route 226
set ip snmp server 228
set ip ssh 228
set ip ssh server 229
set ip telnet 229
set ip telnet server 230
set length 105
set license 106
set load-balancing strictness 447
set location policy 304
set log 764
set log buffer 764
set log console 764
set log current 764
set log mark 767
set log server 764
set log sessions 764
set log trace 764
set mac-user 308
set mac-user attr 309
set mac-usergroup attr 315
set mobility profile 317
set mobility-domain member 30, 332
set mobility-domain mode member seed-ip 333, 334
set mobility-domain mode secondary-seed domain-name 335
set mobility-domain mode seed domain-name 336
set mobility-profile mode 319
set network-domain member seed-ip 346
set network-domain mode seed domain-name 348
set network-domain peer 347
set ntp 231
set ntp server 232
set ntp update-interval 233
set port 137
set port media-type 139
set port mirror 140
set port name 141
set port negotiation 141
set port poe 142
set port speed 143
set port trap 144
set port type ap 145
set port type wired-auth 148
set port-group 138
set prompt 107
set qos cos-to-dscp-map 179
set qos dscp-to-cos-map 180
set qos profile 40
set radio-profile 11n 33
set radio-profile active-scan 448
set radio-profile auto-tune channel-config 450
set radio-profile auto-tune channel-holddown 451
set radio-profile auto-tune channel-interval 452
set radio-profile auto-tune channel-lockdown 453
set radio-profile auto-tune power-config 454
set radio-profile auto-tune power-interval 455
set radio-profile beacon-interval 448, 457
set radio-profile countermeasures 458
set radio-profile dlim-interval 460
set radio-profile frag-threshold 461
set radio-profile long-retry 462
set radio-profile max-rx-lifetime 462
set radio-profile max-tx-lifetime 463
set radio-profile mode 464
set radio-profile preamble-length 467
set radio-profile qos-mode 468
set radio-profile rfd-mode 469
set radio-profile rf-scanning channel-scope 44
set radio-profile rf-scanning mode 43
set radio-profile rts-threshold 469, 471
set radio-profile service-profile 472
set radio-profile short-retry 478
set radio-profile weighted-fair-queuing 41
set radio-profile wmm 478
set radio-profile wmm-powersave 478
set radius 630
set radius client system-ip 632
set radius dac 34
set radius das-port 34
set radius deadtime 630
set radius key 630
set radius proxy client 633
set radius proxy port 634
set radius retransmit 630
set radius server 635
set radius timeout 630
set refetect ssid-list 707
set rfdetect active-scan 700
set rfdetect attack-list 701
set rfdetect black-list 702
set rfdetect classification ad-hoc 45
set rfdetect classification default 46
set rfdetect classification seen-in-network 46
set rfdetect classification ssid-masquerade 47
set rfdetect countermeasures 702
set rfdetect ignore mac 703
set rfdetect log 705
set rfdetect signature 706
set rfdetect signature key 707
set rfdetect ssid-list 45
set rfdetect vendor-list 708
set security acl 600
set security acl hit-sample-rate 607
set security acl ip icmp 600
set security acl ip ip 600
set security acl ip tcp 600
set security acl ip udp 600
set security acl map 605
set security L2-restrict 171
set server group 637
set server group load-balance 638
set service-profile 11n 32
set service-profile attr 479
set service-profile beacon 481
set service-profile auth-dot1x 482
set service-profile auth-psk 483
set service-profile beacon 484
set service-profile bridging 485
set service-profile cac-mode 486
set service-profile cac-session 487
set service-profile cipher-ccmp 488
set service-profile cipher-ccmp 488
set service-profile cipher-tkip 489
set service-profile cipher-wep104 490
set service-profile cipher-wep40 491
set service-profile cos 492
set service-profile dhcp-restrict 493
set service-profile idle-client-probing 494
set service-profile keep-initial-vlan 495
set service-profile load-balancing 496
set service-profile long-retry-count 497
set service-profile max-bw 42
set service-profile no-broadcast 499
set service-profile proxy-arp 500
set service-profile psk-phrase 501
set service-profile psk-raw 502
set service-profile rsn-ie 503
set service-profile shared-key-auth 504
set service-profile short-retry-count 504
set service-profile sda agent-directory 505
set service-profile sda enforce-checks 506
set service-profile sda failure-page 507
set service-profile soda logout-page 508
set service-profile soda mode 510
set service-profile soda remediation-acl 511
set service-profile soda success-page 512
set service-profile ssid-name 513
set service-profile ssid-type 514
set service-profile static-cos 515
set service-profile tkip-mc-time 514
set service-profile transmit-rates 32, 516
set service-profile use-client-dscp 518
set service-profile user-idle-timeout 519
set service-profile web-auth-url 521, 523, 524
set service-profile web-portal-acl 520
set service-profile web-portal-session-timeout 525
set service-profile wip active-multicast-index 526
set service-profile wip active-unicast-index 527
set service-profile wip key-index 528
set service-profile wpa-ie 529
set snmp community 233
set snmp notify profile 235
set snmp notify target 240
set snmp protocol 245
set snmp security 246
set snmp usm 247
set snoop 749
set snoop map 752
set snoop mode 753
set spantree 549
set spantree backbonetop 550
set spantree fwwdelay 551
set spantree hello 551
set spantree maxage 552
set spantree portcost 553
set spantree portfast 554
set spantree portpri 555
set spantree portvancost 556
set spantree portvclan 557
set spantree priority 558
set spantree uplinkf 558
set summertime 250
set system contact 108
set system countrycode 109
set system idle-timeout 113
set system ip-address 114, 251
set system location 115
set system name 116
set timedate 252
set timezone 253
set trace authentication 742
set trace authentication mac-addr 742
set trace authentication port 742
set trace authentication user 742
set trace authorization 743
set trace authorization mac-addr 743
set trace authorization port 743
set trace authorization user  743
set trace dot1x  744
set trace dot1x mac-addr  744
set trace dot1x port  744
set trace dot1x user  744
set trace sm  745
set trace sm mac-addr  745
set trace sm port  745
set trace sm user  745
set user  319
set user attr  321
set user expire-password-in  322
set user group  323
set user password  319
set usergroup  323
set usergroup attr  323
set usergroup expire-password-in  325
set vlan name  172
set vlan port  173
set vlan profile  175
set vlan tunnel-affinity  174
set web-portal  326

T
teinet  254
test  785
test rflink  709
traceroute  255

U
uninstall soda agent  736

V
version  786