The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.


Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.
## Contents

### Configuring AAA

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>1</td>
</tr>
<tr>
<td>RADIUS</td>
<td>2</td>
</tr>
<tr>
<td>HWTACACS</td>
<td>6</td>
</tr>
<tr>
<td>LDAP</td>
<td>9</td>
</tr>
<tr>
<td>AAA implementation on the device</td>
<td>11</td>
</tr>
<tr>
<td>AAA for MPLS L3VPNs</td>
<td>13</td>
</tr>
<tr>
<td>Protocols and standards</td>
<td>13</td>
</tr>
<tr>
<td>RADIUS attributes</td>
<td>14</td>
</tr>
<tr>
<td>FIPS compliance</td>
<td>16</td>
</tr>
<tr>
<td>AAA configuration considerations and task list</td>
<td>17</td>
</tr>
<tr>
<td>Configuring AAA schemes</td>
<td>18</td>
</tr>
<tr>
<td>Configuring local users</td>
<td>18</td>
</tr>
<tr>
<td>Configuring RADIUS schemes</td>
<td>22</td>
</tr>
<tr>
<td>Configuring HWTACACS schemes</td>
<td>33</td>
</tr>
<tr>
<td>Configuring LDAP schemes</td>
<td>40</td>
</tr>
<tr>
<td>Configuring AAA methods for ISP domains</td>
<td>43</td>
</tr>
<tr>
<td>Configuration prerequisites</td>
<td>43</td>
</tr>
<tr>
<td>Creating an ISP domain</td>
<td>43</td>
</tr>
<tr>
<td>Configuring ISP domain attributes</td>
<td>44</td>
</tr>
<tr>
<td>Configuring authentication methods for an ISP domain</td>
<td>44</td>
</tr>
<tr>
<td>Configuring authorization methods for an ISP domain</td>
<td>45</td>
</tr>
<tr>
<td>Configuring accounting methods for an ISP domain</td>
<td>47</td>
</tr>
<tr>
<td>Enabling the session-control feature</td>
<td>48</td>
</tr>
<tr>
<td>Setting the maximum number of concurrent login users</td>
<td>48</td>
</tr>
<tr>
<td>Configuring a NAS-ID profile</td>
<td>48</td>
</tr>
<tr>
<td>Displaying and maintaining AAA</td>
<td>49</td>
</tr>
<tr>
<td>AAA configuration examples</td>
<td>49</td>
</tr>
<tr>
<td>AAA for SSH users by an HWTACACS server</td>
<td>49</td>
</tr>
<tr>
<td>Local authentication, HWTACACS authorization, and RADIUS accounting for SSH users</td>
<td>50</td>
</tr>
<tr>
<td>Authentication and authorization for SSH users by a RADIUS server</td>
<td>52</td>
</tr>
<tr>
<td>Authentication for SSH users by an LDAP server</td>
<td>56</td>
</tr>
<tr>
<td>Troubleshooting RADIUS</td>
<td>61</td>
</tr>
<tr>
<td>RADIUS authentication failure</td>
<td>61</td>
</tr>
<tr>
<td>RADIUS packet delivery failure</td>
<td>61</td>
</tr>
<tr>
<td>RADIUS accounting error</td>
<td>62</td>
</tr>
<tr>
<td>Troubleshooting HWTACACS</td>
<td>62</td>
</tr>
<tr>
<td>Troubleshooting LDAP</td>
<td>62</td>
</tr>
<tr>
<td>LDAP authentication failure</td>
<td>62</td>
</tr>
</tbody>
</table>

### 802.1X overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X architecture</td>
<td>64</td>
</tr>
<tr>
<td>Controlled/uncontrolled port and port authorization status</td>
<td>64</td>
</tr>
<tr>
<td>802.1X-related protocols</td>
<td>64</td>
</tr>
<tr>
<td>Packet formats</td>
<td>65</td>
</tr>
<tr>
<td>EAP over RADIUS</td>
<td>65</td>
</tr>
<tr>
<td>802.1X authentication initiation</td>
<td>66</td>
</tr>
<tr>
<td>802.1X client as the initiator</td>
<td>67</td>
</tr>
<tr>
<td>Access device as the initiator</td>
<td>67</td>
</tr>
<tr>
<td>802.1X authentication procedures</td>
<td>68</td>
</tr>
<tr>
<td>Comparing EAP relay and EAP termination</td>
<td>68</td>
</tr>
<tr>
<td>EAP relay</td>
<td>69</td>
</tr>
<tr>
<td>EAP termination</td>
<td>70</td>
</tr>
</tbody>
</table>

### Configuring 802.1X

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control methods</td>
<td>72</td>
</tr>
<tr>
<td>802.1X VLAN manipulation</td>
<td>72</td>
</tr>
<tr>
<td>Configuring port security</td>
<td>185</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Overview</td>
<td>185</td>
</tr>
<tr>
<td>Port security features</td>
<td>185</td>
</tr>
<tr>
<td>Port security modes</td>
<td>185</td>
</tr>
<tr>
<td>Configuration task list</td>
<td>188</td>
</tr>
<tr>
<td>Enabling port security</td>
<td>188</td>
</tr>
<tr>
<td>Setting port security's limit on the number of secure MAC addresses on a port</td>
<td>189</td>
</tr>
<tr>
<td>Setting the port security mode</td>
<td>189</td>
</tr>
<tr>
<td>Configuring port security features</td>
<td>190</td>
</tr>
<tr>
<td>Configuring NTK</td>
<td>190</td>
</tr>
<tr>
<td>Configuring intrusion protection</td>
<td>191</td>
</tr>
<tr>
<td>Configuring secure MAC addresses</td>
<td>191</td>
</tr>
<tr>
<td>Configuration prerequisites</td>
<td>192</td>
</tr>
<tr>
<td>Configuration procedure</td>
<td>192</td>
</tr>
<tr>
<td>Ignoring authorization information from the server</td>
<td>193</td>
</tr>
<tr>
<td>Enabling MAC move</td>
<td>193</td>
</tr>
<tr>
<td>Applying a NAS-ID profile to port security</td>
<td>194</td>
</tr>
<tr>
<td>Enabling the authorization-fail-offline feature</td>
<td>194</td>
</tr>
<tr>
<td>Enabling SNMP notifications for port security</td>
<td>195</td>
</tr>
<tr>
<td>Displaying and maintaining port security</td>
<td>195</td>
</tr>
<tr>
<td>Port security configuration examples</td>
<td>196</td>
</tr>
<tr>
<td>autoLearn configuration example</td>
<td>196</td>
</tr>
<tr>
<td>userLoginWithOUI configuration example</td>
<td>198</td>
</tr>
<tr>
<td>macAddressElseUserLoginSecure configuration example</td>
<td>201</td>
</tr>
<tr>
<td>Troubleshooting port security</td>
<td>204</td>
</tr>
<tr>
<td>Cannot set the port security mode</td>
<td>204</td>
</tr>
<tr>
<td>Cannot configure secure MAC addresses</td>
<td>205</td>
</tr>
</tbody>
</table>

Configuring password control ........................................... 206

<table>
<thead>
<tr>
<th>Overview</th>
<th>206</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password setting</td>
<td>206</td>
</tr>
<tr>
<td>Password updating and expiration</td>
<td>207</td>
</tr>
<tr>
<td>User login control</td>
<td>208</td>
</tr>
<tr>
<td>Password not displayed in any form</td>
<td>208</td>
</tr>
<tr>
<td>Logging</td>
<td>208</td>
</tr>
<tr>
<td>FIPS compliance</td>
<td>209</td>
</tr>
<tr>
<td>Password control configuration task list</td>
<td>209</td>
</tr>
<tr>
<td>Enabling password control</td>
<td>209</td>
</tr>
<tr>
<td>Setting global password control parameters</td>
<td>210</td>
</tr>
<tr>
<td>Setting user group password control parameters</td>
<td>211</td>
</tr>
<tr>
<td>Setting local user password control parameters</td>
<td>212</td>
</tr>
<tr>
<td>Setting super password control parameters</td>
<td>212</td>
</tr>
<tr>
<td>Displaying and maintaining password control</td>
<td>213</td>
</tr>
</tbody>
</table>
Managing public keys ................................................................. 217

Overview..................................................................................... 217
FIPS compliance......................................................................... 217
Creating a local key pair ............................................................. 217
Distributing a local host public key .............................................. 219
Exporting a host public key ......................................................... 219
Displaying a host public key ......................................................... 219
Destroying a local key pair .......................................................... 220
Configuring a peer host public key .............................................. 220
  Importing a peer host public key from a public key file ............. 220
  Entering a peer host public key .................................................. 221
Displaying and maintaining public keys ...................................... 221
Examples of public key management .......................................... 221
  Example for entering a peer host public key ......................... 221
  Example for importing a public key from a public key file ........ 223

Configuring PKI ........................................................................... 226

Overview..................................................................................... 226
PKI terminology ........................................................................ 226
PKI architecture ........................................................................ 227
PKI operation ............................................................................ 227
PKI applications ........................................................................ 228
Support for MPLS L3VPN ............................................................ 228
FIPS compliance......................................................................... 229
PKI configuration task list .......................................................... 229
Configuring a PKI entity .............................................................. 229
Configuring a PKI domain ........................................................... 230
Requesting a certificate ............................................................... 232
  Configuration guidelines .......................................................... 232
  Configuring automatic certificate request ................................ 233
  Manually requesting a certificate .............................................. 233
Aborting a certificate request ....................................................... 234
Obtaining certificates ................................................................. 234
  Configuration prerequisites ....................................................... 234
  Configuration guidelines .......................................................... 234
  Configuration procedure ......................................................... 235
Verifying PKI certificates ........................................................... 235
  Verifying certificates with CRL checking ................................ 235
  Verifying certificates without CRL checking ......................... 236
Specifying the storage path for the certificates and CRLs .......... 236
Exporting certificates .................................................................. 237
Removing a certificate .................................................................. 237
Configuring a certificate-based access control policy .............. 238
Displaying and maintaining PKI ................................................ 239
PKI configuration examples ....................................................... 239
  Requesting a certificate from an RSA Keon CA server ............ 239
  Requesting a certificate from a Windows Server 2003 CA server 242
  Requesting a certificate from an OpenCA server .................... 245
  Certificate import and export configuration example ............... 248
Troubleshooting PKI configuration ............................................. 253
  Failed to obtain the CA certificate ............................................ 254
  Failed to obtain local certificates ............................................. 254
  Failed to request local certificates .......................................... 255
  Failed to obtain CRLs .............................................................. 255
  Failed to import the CA certificate .......................................... 256
  Failed to import a local certificate ........................................... 257
  Failed to export certificates .................................................... 257
Configuring ND attack defense ............................................................... 477
Configuring MACsec .............................................................................. 461
Enabling MKA ....................................................................................... 465
Enabling MACsec desire ....................................................................... 465
Configuring a preshared key ................................................................. 466
Configuring the MKA key server priority .............................................. 466
Configuring MACsec protection parameters in interface view ............... 467
Configuring the MACsec confidentiality offset ....................................... 467
Configuring MACsec replay protection ............................................... 468
Configuring the MACsec validation mode .............................................. 468
Configuring MACsec protection parameters by MKA policy ................. 468
Configuring an MKA policy ................................................................. 468
Applying an MKA policy .................................................................. 469
Displaying and maintaining MACsec .................................................. 469
MACsec configuration examples ......................................................... 470
Client-oriented MACsec configuration example .................................. 470
Device-oriented MACsec configuration example .................................. 473
Troubleshooting MACsec ................................................................. 476
Configuring user profiles .................................................................. 454
Overview ............................................................................................ 454
Configuration task list ........................................................................ 454
Configuration restrictions and guidelines .......................................... 454
Creating a user profile ....................................................................... 454
Configuring parameters for a user profile .......................................... 454
Configuring QoS parameters for traffic management ......................... 455
Displaying and maintaining user profiles .......................................... 455
User profile configuration examples ................................................. 455
Local 802.1X authentication/authorization with QoS policy configuration example ......................................................... 455
Configuring attack detection and prevention ..................................... 460
Overview ............................................................................................ 460
Configuring TCP fragment attack prevention .................................... 460
Configuring MACsec ........................................................................... 461
Overview ............................................................................................ 461
Basic concepts ................................................................................... 461
MACsec services ................................................................................ 461
MACsec applications ........................................................................ 462
MACsec operating mechanism ........................................................... 462
Protocols and standards ................................................................... 464
Compatibility information ................................................................. 464
Feature and hardware compatibility .................................................... 464
Feature and software version compatibility ....................................... 464
MACsec configuration task list ............................................................ 465
Enabling MKA ................................................................................... 465
Enabling MACsec desire ................................................................... 465
Configuring a preshared key ............................................................... 466
Configuring the MKA key server priority .......................................... 466
Configuring MACsec protection parameters in interface view .......... 467
Configuring the MACsec confidentiality offset .................................... 467
Configuring MACsec replay protection .............................................. 468
Configuring the MACsec validation mode ......................................... 468
Configuring MACsec protection parameters by MKA policy ............ 468
Configuring an MKA policy ............................................................... 468
Applying an MKA policy ................................................................. 469
Displaying and maintaining MACsec ................................................ 469
MACsec configuration examples ........................................................ 470
Client-oriented MACsec configuration example ................................ 470
Device-oriented MACsec configuration example ................................ 473
Troubleshooting MACsec ................................................................. 476
Configuring ND attack defense .......................................................... 477
Overview ............................................................................................ 477
Feature and software version compatibility ........................................ 477
Configuring AAA

Overview

Authentication, Authorization, and Accounting (AAA) provides a uniform framework for implementing network access management. This feature specifies the following security functions:

- **Authentication**—Identifies users and verifies their validity.
- **Authorization**—Grants different users different rights, and controls the users’ access to resources and services. For example, you can permit office users to read and print files and prevent guests from accessing files on the device.
- **Accounting**—Records network usage details of users, including the service type, start time, and traffic. This function enables time-based and traffic-based charging and user behavior auditing.

AAA uses a client/server model. The client runs on the access device, or the network access server (NAS), which authenticates user identities and controls user access. The server maintains user information centrally. See Figure 1.

![Figure 1 AAA network diagram](image)

To access networks or resources beyond the NAS, a user sends its identity information to the NAS. The NAS transparently passes the user information to AAA servers and waits for the authentication, authorization, and accounting result. Based on the result, the NAS determines whether to permit or deny the access request.

AAA has various implementations, including RADIUS, HWTACACS, and LDAP. RADIUS is most often used.

The network in Figure 1 has one RADIUS server and one HWTACACS server. You can use different servers to implement different security functions. For example, you can use the HWTACACS server for authentication and authorization, and use the RADIUS server for accounting.

You can choose the security functions provided by AAA as needed. For example, if your company wants employees to be authenticated before they access specific resources, you would deploy an authentication server. If network usage information is needed, you would also configure an accounting server.

The device performs dynamic password authentication.
RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed information interaction protocol that uses a client/server model. The protocol can protect networks against unauthorized access and is often used in network environments that require both high security and remote user access.

The RADIUS authorization process is combined with the RADIUS authentication process, and user authorization information is piggybacked in authentication responses. RADIUS uses UDP port 1812 for authentication and UDP port 1813 for accounting.

RADIUS was originally designed for dial-in user access, and has been extended to support additional access methods, such as Ethernet and ADSL.

Client/server model

The RADIUS client runs on the NASs located throughout the network. It passes user information to RADIUS servers and acts on the responses to, for example, reject or accept user access requests.

The RADIUS server runs on the computer or workstation at the network center and maintains information related to user authentication and network service access.

The RADIUS server operates using the following process:
1. Receives authentication, authorization, and accounting requests from RADIUS clients.
2. Performs user authentication, authorization, or accounting.
3. Returns user access control information (for example, rejecting or accepting the user access request) to the clients.

The RADIUS server can also act as the client of another RADIUS server to provide authentication proxy services.

The RADIUS server maintains the following databases:
- **Users**—Stores user information, such as the usernames, passwords, applied protocols, and IP addresses.
- **Clients**—Stores information about RADIUS clients, such as shared keys and IP addresses.
- **Dictionary**—Stores RADIUS protocol attributes and their values.

![Figure 2 RADIUS server databases](image)

Information exchange security mechanism

The RADIUS client and server exchange information between them with the help of shared keys, which are preconfigured on the client and server. A RADIUS packet has a 16-byte field called Authenticator. This field includes a signature generated by using the MD5 algorithm, the shared key, and some other information. The receiver of the packet verifies the signature and accepts the packet only when the signature is correct. This mechanism ensures the security of information exchanged between the RADIUS client and server.

The shared keys are also used to encrypt user passwords that are included in RADIUS packets.

User authentication methods

The RADIUS server supports multiple user authentication methods, such as PAP, CHAP, and EAP.
Basic RADIUS packet exchange process

Figure 3 illustrates the interactions between a user host, the RADIUS client, and the RADIUS server.

Figure 3 Basic RADIUS packet exchange process

RADIUS uses the following workflow:

1. The host sends a connection request that includes the user’s username and password to the RADIUS client.
2. The RADIUS client sends an authentication request (Access-Request) to the RADIUS server. The request includes the user’s password, which has been processed by the MD5 algorithm and shared key.
3. The RADIUS server authenticates the username and password. If the authentication succeeds, the server sends back an Access-Accept packet that contains the user’s authorization information. If the authentication fails, the server returns an Access-Reject packet.
4. The RADIUS client permits or denies the user according to the authentication result. If the result permits the user, the RADIUS client sends a start-accounting request (Accounting-Request) packet to the RADIUS server.
5. The RADIUS server returns an acknowledgment (Accounting-Response) packet and starts accounting.
6. The user accesses the network resources.
7. The host requests the RADIUS client to tear down the connection.
8. The RADIUS client sends a stop-accounting request (Accounting-Request) packet to the RADIUS server.
9. The RADIUS server returns an acknowledgment (Accounting-Response) and stops accounting for the user.
10. The RADIUS client notifies the user of the termination.

RADIUS packet format

RADIUS uses UDP to transmit packets. The protocol also uses a series of mechanisms to ensure smooth packet exchange between the RADIUS server and the client. These mechanisms include the timer mechanism, the retransmission mechanism, and the backup server mechanism.
Descriptions of the fields are as follows:

- The Code field (1 byte long) indicates the type of the RADIUS packet. Table 1 gives the main values and their meanings.

Table 1 Main values of the Code field

<table>
<thead>
<tr>
<th>Code</th>
<th>Packet type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Access-Request</td>
<td>From the client to the server. A packet of this type includes user information for the server to authenticate the user. It must contain the User-Name attribute and can optionally contain the attributes of NAS-IP-Address, User-Password, and NAS-Port.</td>
</tr>
<tr>
<td>2</td>
<td>Access-Accept</td>
<td>From the server to the client. If all attribute values included in the Access-Request are acceptable, the authentication succeeds, and the server sends an Access-Accept response.</td>
</tr>
<tr>
<td>3</td>
<td>Access-Reject</td>
<td>From the server to the client. If any attribute value included in the Access-Request is unacceptable, the authentication fails, and the server sends an Access-Reject response.</td>
</tr>
<tr>
<td>4</td>
<td>Accounting-Request</td>
<td>From the client to the server. A packet of this type includes user information for the server to start or stop accounting for the user. The Acct-Status-Type attribute in the packet indicates whether to start or stop accounting.</td>
</tr>
<tr>
<td>5</td>
<td>Accounting-Response</td>
<td>From the server to the client. The server sends a packet of this type to notify the client that it has received the Accounting-Request and has successfully recorded the accounting information.</td>
</tr>
</tbody>
</table>

- The Identifier field (1 byte long) is used to match response packets with request packets and to detect duplicate request packets. The request and response packets of the same exchange process for the same purpose (such as authentication or accounting) have the same identifier.

- The Length field (2 bytes long) indicates the length of the entire packet (in bytes), including the Code, Identifier, Length, Authenticator, and Attributes fields. Bytes beyond this length are considered padding and are ignored by the receiver. If the length of a received packet is less than this length, the packet is dropped.

- The Authenticator field (16 bytes long) is used to authenticate responses from the RADIUS server and to encrypt user passwords. There are two types of authenticators: request authenticator and response authenticator.

- The Attributes field (variable in length) includes authentication, authorization, and accounting information. This field can contain multiple attributes, each with the following subfields:
  - Type—Type of the attribute.
- **Length**—Length of the attribute in bytes, including the Type, Length, and Value subfields.
- **Value**—Value of the attribute. Its format and content depend on the Type subfield.

Commonly used RADIUS attributes are defined in RFC 2865, RFC 2866, RFC 2867, and RFC 2868. For more information, see "Commonly used standard RADIUS attributes."

### Table 2: Commonly used RADIUS attributes

<table>
<thead>
<tr>
<th>No.</th>
<th>Attribute</th>
<th>No.</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>45</td>
<td>Acct-Authentic</td>
</tr>
<tr>
<td>2</td>
<td>User-Password</td>
<td>46</td>
<td>Acct-Session-Time</td>
</tr>
<tr>
<td>3</td>
<td>CHAP-Password</td>
<td>47</td>
<td>Acct-Input-Packets</td>
</tr>
<tr>
<td>4</td>
<td>NAS-IP-Address</td>
<td>48</td>
<td>Acct-Output-Packets</td>
</tr>
<tr>
<td>5</td>
<td>NAS-Port</td>
<td>49</td>
<td>Acct-Terminate-Cause</td>
</tr>
<tr>
<td>6</td>
<td>Service-Type</td>
<td>50</td>
<td>Acct-Multi-Session-Id</td>
</tr>
<tr>
<td>7</td>
<td>Framed-Protocol</td>
<td>51</td>
<td>Acct-Link-Count</td>
</tr>
<tr>
<td>8</td>
<td>Framed-IP-Address</td>
<td>52</td>
<td>Acct-Input-Gigawords</td>
</tr>
<tr>
<td>9</td>
<td>Framed-IP-Netmask</td>
<td>53</td>
<td>Acct-Output-Gigawords</td>
</tr>
<tr>
<td>10</td>
<td>Framed-Routing</td>
<td>54</td>
<td>(unassigned)</td>
</tr>
<tr>
<td>11</td>
<td>Filter-ID</td>
<td>55</td>
<td>Event-Timestamp</td>
</tr>
<tr>
<td>12</td>
<td>Framed-MTU</td>
<td>56-59</td>
<td>(unassigned)</td>
</tr>
<tr>
<td>13</td>
<td>Framed-Compression</td>
<td>60</td>
<td>CHAP-Challenge</td>
</tr>
<tr>
<td>14</td>
<td>Login-IP-Host</td>
<td>61</td>
<td>NAS-Port-Type</td>
</tr>
<tr>
<td>15</td>
<td>Login-Service</td>
<td>62</td>
<td>Port-Limit</td>
</tr>
<tr>
<td>16</td>
<td>Login-TCP-Port</td>
<td>63</td>
<td>Login-LAT-Port</td>
</tr>
<tr>
<td>17</td>
<td>(unassigned)</td>
<td>64</td>
<td>Tunnel-Type</td>
</tr>
<tr>
<td>18</td>
<td>Reply-Message</td>
<td>65</td>
<td>Tunnel-Medium-Type</td>
</tr>
<tr>
<td>19</td>
<td>Callback-Number</td>
<td>66</td>
<td>Tunnel-Client-Endpoint</td>
</tr>
<tr>
<td>20</td>
<td>Callback-ID</td>
<td>67</td>
<td>Tunnel-Server-Endpoint</td>
</tr>
<tr>
<td>21</td>
<td>(unassigned)</td>
<td>68</td>
<td>Acct-Tunnel-Connection</td>
</tr>
<tr>
<td>22</td>
<td>Framed-Route</td>
<td>69</td>
<td>Tunnel-Password</td>
</tr>
<tr>
<td>23</td>
<td>Framed-IPX-Network</td>
<td>70</td>
<td>ARAP-Password</td>
</tr>
<tr>
<td>24</td>
<td>State</td>
<td>71</td>
<td>ARAP-Features</td>
</tr>
<tr>
<td>25</td>
<td>Class</td>
<td>72</td>
<td>ARAP-Zone-Access</td>
</tr>
<tr>
<td>26</td>
<td>Vendor-Specific</td>
<td>73</td>
<td>ARAP-Security</td>
</tr>
<tr>
<td>27</td>
<td>Session-Timeout</td>
<td>74</td>
<td>ARAP-Security-Data</td>
</tr>
<tr>
<td>28</td>
<td>Idle-Timeout</td>
<td>75</td>
<td>Password-Retry</td>
</tr>
<tr>
<td>29</td>
<td>Termination-Action</td>
<td>76</td>
<td>Prompt</td>
</tr>
<tr>
<td>30</td>
<td>Called-Station-Id</td>
<td>77</td>
<td>Connect-Info</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-Id</td>
<td>78</td>
<td>Configuration-Token</td>
</tr>
<tr>
<td>32</td>
<td>NAS-Identifier</td>
<td>79</td>
<td>EAP-Message</td>
</tr>
</tbody>
</table>
Extended RADIUS attributes

The RADIUS protocol features excellent extensibility. The Vendor-Specific attribute (attribute 26) allows a vendor to define extended attributes. The extended attributes implement functions that the standard RADIUS protocol does not provide.

A vendor can encapsulate multiple subattributes in the TLV format in attribute 26 to provide extended functions. As shown in Figure 5, a subattribute encapsulated in attribute 26 consists of the following parts:

- **Vendor-ID**—ID of the vendor. The most significant byte is 0. The other three bytes contains a code compliant to RFC 1700.
- **Vendor-Type**—Type of the subattribute.
- **Vendor-Length**—Length of the subattribute.
- **Vendor-Data**—Contents of the subattribute.

The device supports RADIUS subattributes with a vendor ID of 25506. For more information, see "RADIUS subattributes (vendor ID 25506)."

Figure 5 Format of attribute 26

<table>
<thead>
<tr>
<th>Type</th>
<th>Length</th>
<th>Vendor-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor-ID (continued)</td>
<td>Vendor-Type</td>
<td>Vendor-Length</td>
</tr>
<tr>
<td>Vendor-Data (Specified attribute value……..)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>......</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HWTACACS

HW Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). HWTACACS is similar to RADIUS, and uses a client/server model for information exchange between the NAS and the HWTACACS server.
HWTACACS typically provides AAA services for PPP, VPDN, and terminal users. In a typical HWTACACS scenario, terminal users need to log in to the NAS. Working as the HWTACACS client, the NAS sends users’ usernames and passwords to the HWTACACS server for authentication. After passing authentication and obtaining authorized rights, a user logs in to the device and performs operations. The HWTACACS server records the operations that each user performs.

**Differences between HWTACACS and RADIUS**

HWTACACS and RADIUS have many features in common, such as using a client/server model, using shared keys for data encryption, and providing flexibility and scalability. Table 3 lists the primary differences between HWTACACS and RADIUS.

### Table 3 Primary differences between HWTACACS and RADIUS

<table>
<thead>
<tr>
<th>HWTACACS</th>
<th>RADIUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses TCP, which provides reliable network transmission.</td>
<td>Uses UDP, which provides high transport efficiency.</td>
</tr>
<tr>
<td>Encrypts the entire packet except for the HWTACACS header.</td>
<td>Encrypts only the user password field in an authentication packet.</td>
</tr>
<tr>
<td>Protocol packets are complicated and authorization is independent of authentication. Authorization and authentication can be deployed on different HWTACACS servers.</td>
<td>Protocol packets are simple and the authorization process is combined with the authentication process.</td>
</tr>
<tr>
<td>Supports authorization of configuration commands. Access to commands depends on both the user’s roles and authorization. A user can use only commands that are permitted by the user roles and authorized by the HWTACACS server.</td>
<td>Does not support authorization of configuration commands. Access to commands solely depends on the user's roles. For more information about user roles, see <em>Fundamentals Configuration Guide</em>.</td>
</tr>
</tbody>
</table>

**Basic HWTACACS packet exchange process**

Figure 6 describes how HWTACACS performs user authentication, authorization, and accounting for a Telnet user.
HWTACACS operates using the following workflow:
1. A Telnet user sends an access request to the HWTACACS client.
2. The HWTACACS client sends a start-authentication packet to the HWTACACS server when it receives the request.
3. The HWTACACS server sends back an authentication response to request the username.
4. Upon receiving the response, the HWTACACS client asks the user for the username.
5. The user enters the username.
6. After receiving the username from the user, the HWTACACS client sends the server a continue-authentication packet that includes the username.
7. The HWTACACS server sends back an authentication response to request the login password.
8. Upon receipt of the response, the HWTACACS client prompts the user for the login password.
9. The user enters the password.
10. The HWTACACS client sends the server a continue-authentication packet with the password.
11. Response indicating successful authentication.
13. Response indicating successful authorization.
14. The user logs in successfully.
15. Start-accounting request.
16. Response indicating the start of accounting.
17. The user logs off.
10. After receiving the login password, the HWTACACS client sends the HWTACACS server a continue-authentication packet that includes the login password.

11. If the authentication succeeds, the HWTACACS server sends back an authentication response to indicate that the user has passed authentication.

12. The HWTACACS client sends a user authorization request packet to the HWTACACS server.

13. If the authorization succeeds, the HWTACACS server sends back an authorization response, indicating that the user is now authorized.

14. Knowing that the user is now authorized, the HWTACACS client pushes its CLI to the user and permits the user to log in.

15. The HWTACACS client sends a start-accounting request to the HWTACACS server.

16. The HWTACACS server sends back an accounting response, indicating that it has received the start-accounting request.

17. The user logs off.

18. The HWTACACS client sends a stop-accounting request to the HWTACACS server.

19. The HWTACACS server sends back a stop-accounting response, indicating that the stop-accounting request has been received.

**LDAP**

The Lightweight Directory Access Protocol (LDAP) provides standard multiplatform directory service. LDAP was developed on the basis of the X.500 protocol. It improves the following functions of X.500:

- Read/write interactive access.
- Browse.
- Search.

LDAP is suitable for storing data that does not often change. The protocol is used to store user information. For example, LDAP server software Active Directory Server is used in Microsoft Windows operating systems. The software stores the user information and user group information for user login authentication and authorization.

**LDAP directory service**

LDAP uses directories to maintain the organization information, personnel information, and resource information. The directories are organized in a tree structure and include entries. An entry is a set of attributes with distinguished names (DNs). The attributes are used to store information such as usernames, passwords, emails, computer names, and phone numbers.

LDAP uses a client/server model, and all directory information is stored in the LDAP server. Commonly used LDAP server products include Microsoft Active Directory Server, IBM Tivoli Directory Server, and Sun ONE Directory Server.

**LDAP authentication and authorization**

AAA can use LDAP to provide authentication and authorization services for users. LDAP defines a set of operations to implement its functions. The main operations for authentication and authorization are the bind operation and search operation.

- The bind operation allows an LDAP client to perform the following operations:
  - Establish a connection with the LDAP server.
  - Obtain the access rights to the LDAP server.
  - Check the validity of user information.

- The search operation constructs search conditions and obtains the directory resource information of the LDAP server.

In LDAP authentication, the client completes the following operations:
1. Uses the LDAP server administrator DN to bind with the LDAP server. After the binding is created, the client establishes a connection to the server and obtains the right to search.

2. Constructs search conditions by using the username in the authentication information of a user. The specified root directory of the server is searched and a user DN list is generated.

3. Binds with the LDAP server by using each user DN and password. If a binding is created, the user is considered legal.

In LDAP authorization, the client performs the same operations as in LDAP authentication. When the client constructs search conditions, it obtains both authorization information and the user DN list.

- If the authorization information meets the authorization requirements, the authorization process ends.
- If the authorization information does not meet the authorization requirements, the client sends an administrator bind request to the LDAP server. This operation obtains the right to search for authorization information about users on the user DN list.

Basic LDAP packet exchange process

The following example illustrates the basic packet exchange process during LDAP authentication and authorization for a Telnet user.

**Figure 7 Basic packet exchange process for LDAP authentication of a Telnet user**

The basic packet exchange process is as follows:

1. A Telnet user initiates a connection request and sends the username and password to the LDAP client.
2. After receiving the request, the LDAP client establishes a TCP connection with the LDAP server.
3. To obtain the right to search, the LDAP client uses the administrator DN and password to send an administrator bind request to the LDAP server.
4. The LDAP server processes the request. If the bind operation is successful, the LDAP server sends an acknowledgment to the LDAP client.
5. The LDAP client sends a user DN search request with the username of the Telnet user to the LDAP server.
6. After receiving the request, the LDAP server searches for the user DN by the base DN, search scope, and filtering conditions. If a match is found, the LDAP server sends a response to notify the LDAP client of the successful search. There might be one or more user DNs found.

7. The LDAP client uses the obtained user DN and the entered user password as parameters to send a user DN bind request to the LDAP server. The server will check whether the user password is correct.

8. The LDAP server processes the request, and sends a response to notify the LDAP client of the bind operation result. If the bind operation fails, the LDAP client uses another obtained user DN as the parameter to send a user DN bind request to the LDAP server. This process continues until a DN is bound successfully or all DNs fail to be bound. If all user DNs fail to be bound, the LDAP client notifies the user of the login failure and denies the user's access request.

9. The LDAP client and server perform authorization exchanges. If another scheme (for example, an HWTACACS scheme) is expected for authorization, the LDAP client exchanges authorization packets with the HWTACACS authorization server instead.

10. After successful authorization, the LDAP client notifies the user of the successful login.

### AAA implementation on the device

This section describes AAA user management and methods.

#### User management based on ISP domains and user access types

AAA manages users based on the users' ISP domains and access types.

On a NAS, each user belongs to one ISP domain. The NAS determines the ISP domain to which a user belongs based on the username entered by the user at login.

**Figure 8 Determining the ISP domain for a user by username**

AAA manages users in the same ISP domain based on the users' access types. The device supports the following user access types:

- **LAN**—LAN users must pass 802.1X or MAC authentication to come online.
- **Login**—Login users include SSH, Telnet, FTP, and terminal users who log in to the device. Terminal users can access through console ports.
- **Portal**—Portal users must pass portal authentication to access the network.
- **HTTP or HTTPS**—Users log in to the device through HTTP or HTTPS.

#### NOTE:

The device also provides authentication modules (such as 802.1X) for implementation of user authentication management policies. If you configure these authentication modules, the ISP domains for users of the access types depend on the configuration of the authentication modules.
AAA methods

AAA supports configuring different authentication, authorization, and accounting methods for different types of users in an ISP domain. The NAS determines the ISP domain and access type of a user. The NAS also uses the methods configured for the access type in the domain to control the user's access.

AAA also supports configuring a set of default methods for an ISP domain. These default methods are applied to users for whom no AAA methods are configured.

The device supports the following authentication methods:

- **No authentication**—This method trusts all users and does not perform authentication. For security purposes, do not use this method.
- **Local authentication**—The NAS authenticates users by itself, based on the locally configured user information including the usernames, passwords, and attributes. Local authentication allows high speed and low cost, but the amount of information that can be stored is limited by the size of the storage space.
- **Remote authentication**—The NAS works with a RADIUS, HWTACACS, or LDAP server to authenticate users. The server manages user information in a centralized manner. Remote authentication provides high capacity, reliable, and centralized authentication services for multiple NASs. You can configure backup methods to be used when the remote server is not available.

The device supports the following authorization methods:

- **No authorization**—The NAS performs no authorization exchange. The following default authorization information applies after users pass authentication:
  - Non-login users can access the network.
  - Login users are assigned the default user role. For more information about the default user role feature, see *Fundamentals Configuration Guide*.
  - The working directory for FTP, SFTP, and SCP login users is the root directory of the NAS. However, the users do not have permission to access the root directory.
- **Local authorization**—The NAS performs authorization according to the user attributes locally configured for users.
- **Remote authorization**—The NAS works with a RADIUS, HWTACACS, or LDAP server to authorize users. RADIUS authorization is bound with RADIUS authentication. RADIUS authorization can work only after RADIUS authentication is successful, and the authorization information is included in the Access-Accept packet. HWTACACS authorization is separate from HWTACACS authentication, and the authorization information is included in the authorization response after successful authentication. You can configure backup methods to be used when the remote server is not available.

The device supports the following accounting methods:

- **No accounting**—The NAS does not perform accounting for the users.
- **Local accounting**—Local accounting is implemented on the NAS. It counts and controls the number of concurrent users who use the same local user account, but does not provide statistics for charging.
- **Remote accounting**—The NAS works with a RADIUS server or HWTACACS server for accounting. You can configure backup methods to be used when the remote server is not available.

In addition, the device provides the following login services to enhance device security:

- **Command authorization**—Enables the NAS to let the authorization server determine whether a command entered by a login user is permitted. Login users can execute only commands permitted by the authorization server. For more information about command authorization, see *Fundamentals Configuration Guide*.
• **Command accounting**—When command authorization is disabled, command accounting enables the accounting server to record all valid commands executed on the device. When command authorization is enabled, command accounting enables the accounting server to record all authorized commands. For more information about command accounting, see *Fundamentals Configuration Guide*.

• **User role authentication**—Authenticates each user who wants to obtain another user role without logging out or getting disconnected. For more information about user role authentication, see *Fundamentals Configuration Guide*.

### AAA for MPLS L3VPNs

You can deploy AAA across VPNs in an MPLS L3VPN scenario where clients in different VPNs are centrally authenticated. The deployment enables forwarding of RADIUS and HWTACACS packets across MPLS VPNs. For example, as shown in Figure 9, you can deploy AAA across the VPNs. The PE at the left side of the MPLS backbone acts as a NAS. The NAS transparently delivers the AAA packets of private users in VPN 1 and VPN 2 to the AAA servers in VPN 3 for centralized authentication. Authentication packets of private users in different VPNs do not affect each other.

**Figure 9 Network diagram**

This feature can also help an MCE to implement portal authentication for VPNs. For more information about MCE, see *MPLS Configuration Guide*. For more information about portal authentication, see "Configuring portal authentication."

### Protocols and standards

- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*
- RFC 1492, *An Access Control Protocol, Sometimes Called TACACS*
### RADIUS attributes

#### Commonly used standard RADIUS attributes

<table>
<thead>
<tr>
<th>No.</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User-Name</td>
<td>Name of the user to be authenticated.</td>
</tr>
<tr>
<td>2</td>
<td>User-Password</td>
<td>User password for PAP authentication, only present in Access-Request packets when PAP authentication is used.</td>
</tr>
<tr>
<td>3</td>
<td>CHAP-Password</td>
<td>Digest of the user password for CHAP authentication, only present in Access-Request packets when CHAP authentication is used.</td>
</tr>
<tr>
<td>4</td>
<td>NAS-IP-Address</td>
<td>IP address for the server to use to identify the client. Typically, a client is identified by the IP address of its access interface. This attribute is only present in Access-Request packets.</td>
</tr>
<tr>
<td>5</td>
<td>NAS-Port</td>
<td>Physical port of the NAS that the user accesses.</td>
</tr>
<tr>
<td>6</td>
<td>Service-Type</td>
<td>Type of service that the user has requested or type of service to be provided.</td>
</tr>
<tr>
<td>7</td>
<td>Framed-Protocol</td>
<td>Encapsulation protocol for framed access.</td>
</tr>
<tr>
<td>8</td>
<td>Framed-IP-Address</td>
<td>IP address assigned to the user.</td>
</tr>
<tr>
<td>11</td>
<td>Filter-ID</td>
<td>Name of the filter list.</td>
</tr>
<tr>
<td>12</td>
<td>Framed-MTU</td>
<td>MTU for the data link between the user and NAS. For example, with 802.1X EAP authentication, NAS uses this attribute to notify the server of the MTU for EAP packets to avoid oversized EAP packets.</td>
</tr>
<tr>
<td>14</td>
<td>Login-IP-Host</td>
<td>IP address of the NAS interface that the user accesses.</td>
</tr>
<tr>
<td>15</td>
<td>Login-Service</td>
<td>Type of the service that the user uses for login.</td>
</tr>
<tr>
<td>18</td>
<td>Reply-Message</td>
<td>Text to be displayed to the user, which can be used by the server to communicate information, for example, the reason of the authentication failure.</td>
</tr>
<tr>
<td>26</td>
<td>Vendor-Specific</td>
<td>Vendor-specific proprietary attribute. A packet can contain one or more proprietary attributes, each of which can contain one or more subattributes.</td>
</tr>
<tr>
<td>27</td>
<td>Session-Timeout</td>
<td>Maximum service duration for the user before termination of the session.</td>
</tr>
<tr>
<td>28</td>
<td>Idle-Timeout</td>
<td>Maximum idle time permitted for the user before termination of the session.</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-Id</td>
<td>User identification that the NAS sends to the server. For the LAN access service provided by an HPE device, this attribute includes the MAC address of the user in the format HH-HH-HH-HH-HH-HH.</td>
</tr>
<tr>
<td>32</td>
<td>NAS-Identifier</td>
<td>Identification that the NAS uses to identify itself to the RADIUS server.</td>
</tr>
</tbody>
</table>
| 40  | Acct-Status-Type     | Type of the Accounting-Request packet. Possible values include:  
  - 1—Start.  
  - 2—Stop.  
  - 3—Interim-Update.  
  - 4—Reset-Charge.  
  - 7—Accounting-On. (Defined in the 3rd Generation Partnership Project.)  
  - 8—Accounting-Off. (Defined in the 3rd Generation Partnership Project.)  
  - 9 to 14—Reserved for tunnel accounting.  
  - 15—Reserved for failed. |
<table>
<thead>
<tr>
<th>No.</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>Acct-Authentic</td>
<td>Authentication method used by the user. Possible values include: • 1—RADIUS. • 2—Local. • 3—Remote.</td>
</tr>
<tr>
<td>60</td>
<td>CHAP-Challenge</td>
<td>CHAP challenge generated by the NAS for MD5 calculation during CHAP authentication.</td>
</tr>
<tr>
<td>61</td>
<td>NAS-Port-Type</td>
<td>Type of the physical port of the NAS that is authenticating the user. Possible values include: • 15—Ethernet. • 16—Any type of ADSL. • 17—Cable. (With cable for cable TV.) • 19—WLAN-IEEE 802.11. • 201—VLAN. • 202—ATM. If the port is an ATM or Ethernet one and VLANs are implemented on it, the value of this attribute is 201.</td>
</tr>
<tr>
<td>79</td>
<td>EAP-Message</td>
<td>Used to encapsulate EAP packets to allow RADIUS to support EAP authentication.</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
<td>Used for authentication and verification of authentication packets to prevent spoofing Access-Requests. This attribute is present when EAP authentication is used.</td>
</tr>
<tr>
<td>87</td>
<td>NAS-Port-Id</td>
<td>String for describing the port of the NAS that is authenticating the user.</td>
</tr>
</tbody>
</table>

**RADIUS subattributes (vendor ID 25506)**

<table>
<thead>
<tr>
<th>No.</th>
<th>Subattribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Input-Peak-Rate</td>
<td>Peak rate in the direction from the user to the NAS, in bps.</td>
</tr>
<tr>
<td>2</td>
<td>Input-Average-Rate</td>
<td>Average rate in the direction from the user to the NAS, in bps.</td>
</tr>
<tr>
<td>3</td>
<td>Input-Basic-Rate</td>
<td>Basic rate in the direction from the user to the NAS, in bps.</td>
</tr>
<tr>
<td>4</td>
<td>Output-Peak-Rate</td>
<td>Peak rate in the direction from the NAS to the user, in bps.</td>
</tr>
<tr>
<td>5</td>
<td>Output-Average-Rate</td>
<td>Average rate in the direction from the NAS to the user, in bps.</td>
</tr>
<tr>
<td>6</td>
<td>Output-Basic-Rate</td>
<td>Basic rate in the direction from the NAS to the user, in bps.</td>
</tr>
<tr>
<td>15</td>
<td>Remanent_Volume</td>
<td>Total amount of data available for the connection, in different units for different server types.</td>
</tr>
<tr>
<td>20</td>
<td>Command</td>
<td>Operation for the session, used for session control. Possible values include: • 1—Trigger-Request. • 2—Terminate-Request. • 3—SetPolicy. • 4—Result. • 5—PortalClear.</td>
</tr>
<tr>
<td>24</td>
<td>Control_Identifier</td>
<td>Identification for retransmitted packets. For retransmitted packets from the same session, this attribute must be the same value. For retransmitted packets from different sessions, this attribute does not have to be the same value. The client response of a retransmitted packet must also include this attribute and the value of this attribute must be the same. For Accounting-Request packets of the start, stop, and interim update</td>
</tr>
<tr>
<td>No.</td>
<td>Subattribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>25</td>
<td>Result_Code</td>
<td>Result of the Trigger-Request or SetPolicy operation, zero for success and any other value for failure.</td>
</tr>
<tr>
<td>26</td>
<td>Connect_ID</td>
<td>Index of the user connection.</td>
</tr>
<tr>
<td>28</td>
<td>Ftp_Directory</td>
<td>FTP, SFTP, or SCP user working directory. When the RADIUS client acts as the FTP, SFTP, or SCP server, this attribute is used to set the working directory for an FTP, SFTP, or SCP user on the RADIUS client.</td>
</tr>
<tr>
<td>29</td>
<td>Exec_Privilege</td>
<td>EXEC user priority.</td>
</tr>
<tr>
<td>59</td>
<td>NAS_Startup_Timestamp</td>
<td>Startup time of the NAS in seconds, which is represented by the time elapsed after 00:00:00 on Jan. 1, 1970 (UTC).</td>
</tr>
<tr>
<td>60</td>
<td>Ip_Host_Addr</td>
<td>User IP address and MAC address included in authentication and accounting requests, in the format A.B.C.D hh:hh:hh:hh:hh:hh. A space is required between the IP address and the MAC address.</td>
</tr>
<tr>
<td>61</td>
<td>User_Notify</td>
<td>Information that must be sent from the server to the client transparently.</td>
</tr>
<tr>
<td>62</td>
<td>User_HeartBeat</td>
<td>Hash value assigned after an 802.1X user passes authentication, which is a 32-byte string. This attribute is stored in the user list on the NAS and verifies the handshake packets from the 802.1X user. This attribute only exists in Access-Accept and Accounting-Request packets.</td>
</tr>
<tr>
<td>140</td>
<td>User_Group</td>
<td>User groups assigned after the SSL VPN user passes authentication. A user can belong to multiple user groups that are separated by semicolons. This attribute is used to work with the SSL VPN device.</td>
</tr>
<tr>
<td>141</td>
<td>Security_Level</td>
<td>Security level assigned after the SSL VPN user passes security authentication.</td>
</tr>
<tr>
<td>201</td>
<td>Input-Interval-Octets</td>
<td>Number of bytes input within a realtime accounting interval.</td>
</tr>
<tr>
<td>202</td>
<td>Output-Interval-Octets</td>
<td>Number of bytes output within a realtime accounting interval.</td>
</tr>
<tr>
<td>203</td>
<td>Input-Interval-Packets</td>
<td>Number of packets input within an accounting interval in the unit set on the NAS.</td>
</tr>
<tr>
<td>204</td>
<td>Output-Interval-Packets</td>
<td>Number of packets output within an accounting interval in the unit set on the NAS.</td>
</tr>
<tr>
<td>205</td>
<td>Input-Interval-Gigawords</td>
<td>Amount of bytes input within an accounting interval, in units of 4G bytes.</td>
</tr>
<tr>
<td>206</td>
<td>Output-Interval-Gigawords</td>
<td>Amount of bytes output within an accounting interval, in units of 4G bytes.</td>
</tr>
<tr>
<td>207</td>
<td>Backup-NAS-IP</td>
<td>Backup source IP address for sending RADIUS packets.</td>
</tr>
<tr>
<td>255</td>
<td>Product_ID</td>
<td>Product name.</td>
</tr>
</tbody>
</table>

**FIPS compliance**

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see “Configuring FIPS”) and non-FIPS mode.
AAA configuration considerations and task list

To configure AAA, complete the following tasks on the NAS:

1. Configure the required AAA schemes.
   - **Local authentication**—Configure local users and the related attributes, including the usernames and passwords, for the users to be authenticated.
   - **Remote authentication**—Configure the required RADIUS, HWTACACS, and LDAP schemes.

2. Configure AAA methods for the users' ISP domains. To use remote AAA methods, you must specify the configured RADIUS, HWTACACS, or LDAP schemes in the ISP domains.

**Figure 10 AAA configuration procedure**

To configure AAA, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Perform at least one of the following tasks to configure local users or AAA schemes:</td>
</tr>
<tr>
<td>• Configuring local users</td>
</tr>
<tr>
<td>• Configuring RADIUS schemes</td>
</tr>
<tr>
<td>• Configuring HWTACACS schemes</td>
</tr>
<tr>
<td>• Configuring LDAP schemes</td>
</tr>
<tr>
<td>(Required.) Configure AAA methods for ISP domains:</td>
</tr>
<tr>
<td>1. <strong>(Required.)</strong> Creating an ISP domain</td>
</tr>
<tr>
<td>2. <strong>(Optional.)</strong> Configuring ISP domain attributes</td>
</tr>
<tr>
<td>3. <strong>(Required.)</strong> Perform at least one of the following tasks to configure AAA authentication, authorization, and accounting methods for the ISP domain:</td>
</tr>
<tr>
<td>- Configuring authentication methods for an ISP domain</td>
</tr>
<tr>
<td>- Configuring authorization methods for an ISP domain</td>
</tr>
<tr>
<td>- Configuring accounting methods for an ISP domain</td>
</tr>
<tr>
<td>(Optional.) Enabling the session-control feature</td>
</tr>
<tr>
<td>(Optional.) Setting the maximum number of concurrent login users</td>
</tr>
<tr>
<td>(Optional.) Configuring a NAS-ID profile</td>
</tr>
</tbody>
</table>
Configuring AAA schemes

This section includes information on configuring local users, RADIUS schemes, HWTACACS schemes, and LDAP schemes.

Configuring local users

To implement local authentication, authorization, and accounting, create local users and configure user attributes on the device. The local users and attributes are stored in the local user database on the device. A local user is uniquely identified by the combination of a username and a user type. Local users are classified into the following types:

- **Device management user**—User who logs in to the device for device management.
- **Network access user**—User who accesses network resources through the device.

The following shows the configurable local user attributes:

- **Service type**—Services that the user can use. Local authentication checks the service types of a local user. If none of the service types is available, the user cannot pass authentication. Service types include FTP, HTTP, HTTPS, LAN access, portal, SSH, Telnet, and terminal.
- **User state**—There are two user states: active and blocked. A user in active state can request network services. A user in blocked state cannot request authentication, authorization, and accounting services, but it can request to stop the accounting service in use.
- **Upper limit of concurrent logins using the same user name**—Maximum number of users who can concurrently access the device by using the same user name. When the number reaches the upper limit, no more local users can access the device by using the user name.
- **User group**—Each local user belongs to a local user group and has all attributes of the group. The attributes include the password control attributes and authorization attributes. For more information about local user group, see "Configuring user group attributes."
- **Binding attributes**—Binding attributes control the scope of users, and are checked during local authentication of a user. If the attributes of a user do not match the binding attributes configured for the local user account, the user cannot pass authentication. Binding attributes include the IP address, access port, MAC address, and native VLAN. For support and usage information about binding attributes, see "Configuring local user attributes."
- **Authorization attributes**—Authorization attributes indicate the user's rights after it passes local authentication. Authorization attributes include the ACL, idle cut feature, user profile, user role, VLAN, and FTP/SFTP/SCP working directory. For support information about authorization attributes, see "Configuring local user attributes."

Configure the authorization attributes based on the service type of local users.

You can configure an authorization attribute in user group view or local user view. The setting of an authorization attribute in local user view takes precedence over the attribute setting in user group view.

- The attribute configured in user group view takes effect on all local users in the user group.
- The attribute configured in local user view takes effect only on the local user.

- **Password control attributes**—Password control attributes help control password security for device management users. Password control attributes include password aging time, minimum password length, password composition checking, password complexity checking, and login attempt limit.

You can configure a password control attribute in system view, user group view, or local user view. A password control attribute with a smaller effective range has a higher priority. For more information about password management and global password configuration, see "Configuring password control."
Local user configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring local user attributes</td>
</tr>
<tr>
<td>(Optional.) Configuring user group attributes</td>
</tr>
<tr>
<td>(Optional.) Displaying and maintaining local users and local user groups</td>
</tr>
</tbody>
</table>

Configuring local user attributes

When you configure local user attributes, follow these guidelines:

- When you use the `password-control enable` command to globally enable the password control feature, local user passwords are not displayed.
- You can configure authorization attributes and password control attributes in local user view or user group view. The setting in local user view takes precedence over the setting in user group view.
- Configure authorization attributes according to the application environments and purposes. Support for authorization attributes depends on the service types of users.
  - For LAN and portal users, only the following authorization attributes are effective: `acl`, `user-profile`, and `vlan`.
  - For HTTP and HTTPS users, only the authorization attribute `user-role` is effective.
  - For Telnet and terminal users, only the following authorization attributes are effective: `idle-cut` and `user-role`.
  - For SSH users, only the following authorization attributes are effective: `idle-cut`, `user-role`, and `work-directory`.
  - For FTP users, only the following authorization attributes are effective: `user-role` and `work-directory`.
  - For other types of local users, no authorization attribute is effective.
- Configure the `location` binding attribute based on the service types of users.
  - For 802.1X users, specify the 802.1X-enabled Layer 2 Ethernet interfaces through which the users access the device.
  - For MAC authentication users, specify the MAC authentication-enabled Layer 2 Ethernet interfaces through which the users access the device.
  - For portal users, specify the portal-enabled interfaces through which the users access the device. Specify the Layer 2 Ethernet interfaces if portal is enabled on VLAN interfaces and the `portal roaming enable` command is not configured.

To configure local user attributes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Add a local user and enter local user view.</td>
<td>By default, no local user exists.</td>
</tr>
<tr>
<td></td>
<td>local-user user-name [ class { manage</td>
<td>network } ]</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Configure a password for the local user.</td>
<td>Network access user passwords are encrypted with the encryption algorithm and saved in ciphertext. Device management user passwords are encrypted with the hash algorithm and saved in ciphertext. In non-FIPS mode, a non-password-protected user passes authentication if the user</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>4.</td>
<td>Assign services to the local user.</td>
<td>By default, no service is authorized to a local user.</td>
</tr>
<tr>
<td></td>
<td>For a network access user:</td>
<td>By default, no service is authorized to a local user.</td>
</tr>
<tr>
<td></td>
<td>service-type { lan-access</td>
<td>portal }</td>
</tr>
<tr>
<td></td>
<td>For a device management user:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o In non-FIPS mode:</td>
<td>By default, no service is authorized to a local user.</td>
</tr>
<tr>
<td></td>
<td>service-type { ftp</td>
<td>( http</td>
</tr>
<tr>
<td></td>
<td>o In FIPS mode:</td>
<td>By default, no service is authorized to a local user.</td>
</tr>
<tr>
<td></td>
<td>service-type { https</td>
<td>ssh</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Place the local user to the active or blocked state.</td>
<td>By default, a created local user is in active state and can request network services.</td>
</tr>
<tr>
<td></td>
<td>state { active</td>
<td>block }</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Set the upper limit of concurrent logins using the local user name.</td>
<td>By default, the number of concurrent logins is not limited for the local user.</td>
</tr>
<tr>
<td></td>
<td>access-limit max-user-number</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>(Optional.) Configure binding attributes for the local user.</td>
<td>By default, no binding attribute is configured for a local user.</td>
</tr>
<tr>
<td></td>
<td>bind-attribute { ip ip-address</td>
<td>location interface interface-type interface-number</td>
</tr>
<tr>
<td>8.</td>
<td>(Optional.) Configure authorization attributes for the local user.</td>
<td>The following default settings apply:</td>
</tr>
<tr>
<td></td>
<td>authorization-attribute { acl acl-number</td>
<td>idle-cut minute</td>
</tr>
<tr>
<td></td>
<td>o Set the password aging time:</td>
<td>The following default settings apply:</td>
</tr>
<tr>
<td></td>
<td>password-control aging aging-time</td>
<td>The following default settings apply:</td>
</tr>
<tr>
<td></td>
<td>o Set the minimum password length:</td>
<td>The following default settings apply:</td>
</tr>
<tr>
<td></td>
<td>password-control length length</td>
<td>The following default settings apply:</td>
</tr>
</tbody>
</table>

Optional. | By default, the local user uses password control attributes of the user group to which the local user belongs. Only device management users support the password control.
### Configuring User Group Attributes

User groups simplify local user configuration and management. A user group contains a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized user attributes management for the local users in the group. Local user attributes that are manageable include authorization attributes.

By default, every new local user belongs to the default user group `system` and has all attributes of the group. To assign a local user to a different user group, use the `group` command in local user view.

To configure user group attributes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a user group and enter user group view.</td>
<td>user-group group-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure authorization attributes for the user group.</td>
<td>authorization-attribute { acl acl-number</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure password control attributes for the user group.</td>
<td></td>
</tr>
</tbody>
</table>

---

**Table:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Configure the password composition policy:</td>
<td>feature.</td>
</tr>
<tr>
<td></td>
<td><code>password-control composition type-number</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>type-number [ type-length type-length ]</code></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Configure the password complexity checking policy:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>password-control complexity</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>`{ same-character</td>
<td>user-name } check`</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the maximum login attempts and the action to take if there is a login failure:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>password-control login-attempt login-times</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>`[ exceed { lock</td>
<td>lock-time time</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Assign the local user to a user group.</td>
<td>group group-name</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>

- Configure the password complexity checking policy:
  `password-control complexity { same-character | user-name } check`
- Configure the maximum login attempts and the action to take for login failures:
  `password-control login-attempt { login-times exceed { lock | lock-time time | unlock } }

Displaying and maintaining local users and local user groups

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the local user configuration and online user statistics.</td>
<td>`display local-user [ class { manage</td>
</tr>
<tr>
<td>Display the user group configuration.</td>
<td><code>display user-group [ group-name ]</code></td>
</tr>
</tbody>
</table>

Configuring RADIUS schemes

A RADIUS scheme specifies the RADIUS servers that the device can work with and defines a set of parameters. The device uses the parameters to exchange information with the RADIUS servers, including the server IP addresses, UDP port numbers, shared keys, and server types.

Configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Configuring a test profile for RADIUS server status detection</td>
</tr>
<tr>
<td>(Required.) Creating a RADIUS scheme</td>
</tr>
<tr>
<td>(Required.) Specifying the RADIUS authentication servers</td>
</tr>
<tr>
<td>(Optional.) Specifying the RADIUS accounting servers and the relevant parameters</td>
</tr>
<tr>
<td>(Optional.) Specifying the shared keys for secure RADIUS communication</td>
</tr>
<tr>
<td>(Optional.) Specifying a VPN for the scheme</td>
</tr>
<tr>
<td>(Optional.) Setting the username format and traffic statistics units</td>
</tr>
<tr>
<td>(Optional.) Setting the maximum number of RADIUS request transmission attempts</td>
</tr>
<tr>
<td>(Optional.) Setting the status of RADIUS servers</td>
</tr>
<tr>
<td>(Optional.) Enabling the RADIUS server load sharing feature</td>
</tr>
<tr>
<td>(Optional.) Specifying the source IP address for outgoing RADIUS packets</td>
</tr>
<tr>
<td>(Optional.) Setting RADIUS timers</td>
</tr>
<tr>
<td>(Optional.) Configuring the accounting-on feature</td>
</tr>
</tbody>
</table>
Tasks at a glance
(Optional.) Configuring the IP addresses of the security policy servers
(Optional.) Configuring the Login-Service attribute check method for SSH, FTP, and terminal users
(Optional.) Enabling SNMP notifications for RADIUS
(Optional.) Displaying and maintaining RADIUS

Configuring a test profile for RADIUS server status detection

**IMPORTANT:**
This feature is available in Release 1121 and later.

Use a test profile to detect whether a RADIUS authentication server is reachable at a detection interval. To detect the RADIUS server status, you must configure the RADIUS server to use this test profile in a RADIUS scheme.

With the test profile specified, the device sends a detection packet to the RADIUS server within each detection interval. The detection packet is a simulated authentication request that includes the specified username and password in the test profile.

- If the device receives a response from the server within the interval, it sets the server to the active state.
- If the device does not receive any response from the server within the interval, it sets the server to the blocked state.

The device refreshes the RADIUS server status at each detection interval according to the detection result.

The device stops detecting the status of the RADIUS server when one of the following operations is performed:

- The RADIUS server is removed from the RADIUS scheme.
- The test profile configuration is removed for the RADIUS server in RADIUS scheme view.
- The test profile is deleted.
- The RADIUS server is manually set to the blocked state.
- The RADIUS scheme is deleted.

To configure a test profile for RADIUS server status detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>6. Configure a test profile for detecting the status of RADIUS authentication servers.</td>
<td>radius-server test-profile profile-name username name [ password { cipher</td>
<td>simple } string ] [ interval interval ]</td>
</tr>
</tbody>
</table>

Creating a RADIUS scheme

Create a RADIUS scheme before performing any other RADIUS configurations. You can configure a maximum of 16 RADIUS schemes. A RADIUS scheme can be used by multiple ISP domains.

To create a RADIUS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Specifying the RADIUS authentication servers

A RADIUS authentication server completes authentication and authorization together, because authorization information is piggybacked in authentication responses sent to RADIUS clients.

You can specify one primary authentication server and a maximum of 16 secondary authentication servers for a RADIUS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. A RADIUS authentication server can act as the primary authentication server for one scheme and a secondary authentication server for another scheme at the same time.

When RADIUS server load sharing is enabled, the device distributes the workload over all servers without considering the primary and secondary server roles. The device checks the weight value and number of currently served users for each active server, and then determines the most appropriate server in performance to receive an authentication request.

To specify a RADIUS server by hostname in an MPLS VPN network, first complete one of the following tasks on the device:

- Configure hostname-to-IP address mappings for the VPN by using the `ip host` or `ipv6 host` command.
- Configure a DNS server for the VPN by using the `dns server` or `ipv6 dns server` command.

For more information about these commands, see *Layer 3—IP Services Command Reference*.

To specify RADIUS authentication servers for a RADIUS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Create a RADIUS scheme and enter RADIUS scheme view.</td>
<td></td>
</tr>
</tbody>
</table>
|      | `radius scheme radius-scheme-name` | The default setting depends on the type of the startup configuration:  
- If the device starts up with initial settings, no RADIUS scheme is defined.  
- If the device starts up with the factory defaults, a RADIUS scheme named `system` is defined.  
For more information about the startup configuration, see *Fundamentals Configuration Guide*. |

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td><code>radius scheme radius-scheme-name</code></td>
</tr>
</tbody>
</table>
| 3.   | Specify RADIUS authentication servers. | - Specify the primary RADIUS authentication server: `primary authentication { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | test-profile profile-name | vpn-instance vpn-instance-name | weight weight-value ] *`  
- Specify a secondary RADIUS authentication server:  
  - By default, no authentication server is specified.  
  - Two authentication servers in a scheme, primary or secondary, cannot have the same combination of hostname, IP address, port number, and VPN.  
  - The `weight weight-value` option takes effect only when the RADIUS server load sharing feature is enabled. |
### Specifying the RADIUS accounting servers and the relevant parameters

You can specify one primary accounting server and a maximum of 16 secondary accounting servers for a RADIUS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. A RADIUS accounting server can act as the primary accounting server for one scheme and a secondary accounting server for another scheme at the same time.

When RADIUS server load sharing is enabled, the device distributes the workload over all servers without considering the primary and secondary server roles. The device checks the weight value and number of currently served users for each active server, and then determines the most appropriate server in performance to receive an accounting request.

The device sends a stop-accounting request to the accounting server in the following situations:

- The device receives a connection teardown request from a host.
- The device receives a connection teardown command from an administrator.

When the maximum number of realtime accounting attempts is reached, the device disconnects users who have no accounting responses.

RADIUS does not support accounting for FTP, SFTP, and SCP users.

To specify a RADIUS server by hostname in an MPLS VPN network, first complete one of the following tasks on the device:

- Configure hostname-to-IP address mappings for the VPN by using the `ip host` or `ipv6 host` command.
- Configure a DNS server for the VPN by using the `dns server` or `ipv6 dns server` command.

For more information about these commands, see *Layer 3—IP Services Command Reference*.

To specify RADIUS accounting servers and the relevant parameters for a RADIUS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td>radius scheme radius-scheme-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify RADIUS accounting servers.</td>
<td>primary accounting { host-name</td>
</tr>
</tbody>
</table>
**Specifying the shared keys for secure RADIUS communication**

The RADIUS client and server use the MD5 algorithm and shared keys to generate the Authenticator value for packet authentication and user password encryption. The client and server must use the same key for each type of communication.

A key configured in this task is for all servers of the same type (accounting or authentication) in the scheme. The key has a lower priority than a key configured individually for a RADIUS server.

To specify a shared key for secure RADIUS communication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td>radius-view radius-scheme-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify a shared key for secure RADIUS communication.</td>
<td>key { accounting</td>
</tr>
</tbody>
</table>

**Specifying a VPN for the scheme**

The VPN specified for a RADIUS scheme applies to all authentication and accounting servers in that scheme. If a VPN is also configured for an individual RADIUS server, the VPN specified for the RADIUS scheme does not take effect on that server.

To specify a VPN for a scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td>radius-view radius-scheme-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify a VPN for the RADIUS scheme.</td>
<td>vpn-instance vpn-instance-name</td>
</tr>
</tbody>
</table>

**Setting the username format and traffic statistics units**

A username is in the `userid@isp-name` format, where the `isp-name` argument represents the user's ISP domain name. By default, the ISP domain name is included in a username. However, older RADIUS servers might not recognize usernames that contain the ISP domain names. In this case, you can configure the device to remove the domain name of each username to be sent.

If two or more ISP domains use the same RADIUS scheme, configure the RADIUS scheme to keep the ISP domain name in usernames for domain identification.
The device reports online user traffic statistics in accounting packets. The traffic measurement units are configurable, but they must be the same as the traffic measurement units configured on the RADIUS accounting servers.

To set the username format and the traffic statistics units for a RADIUS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>radius scheme radius-scheme-name</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 3.   | user-name-format { keep-original | with-domain | without-domain } | The default setting depends on the type of the startup configuration:  
• If the device starts up with initial settings, the ISP domain name is included in a username.  
• If the device starts up with the factory defaults, the ISP domain name is included in a username except for the predefined RADIUS scheme named system. When the username is sent to a RADIUS server in the system scheme, the ISP domain name is removed.  
For more information about the startup configuration, see Fundamentals Configuration Guide. |
| 4.   | data-flow-format { data ( byte | giga-byte | kilo-byte | mega-byte ) | packet ( giga-packet | kilo-packet | mega-packet | one-packet ) } | By default, traffic is counted in bytes and packets. |

Setting the maximum number of RADIUS request transmission attempts

RADIUS uses UDP packets to transfer data. Because UDP communication is not reliable, RADIUS uses a retransmission mechanism to improve reliability. A RADIUS request is retransmitted if the NAS does not receive a server response for the request within the response timeout timer. For more information about the RADIUS server response timeout timer, see "Setting RADIUS timers."

You can set the maximum number for the NAS to retransmit a RADIUS request to the same server. When the maximum number is reached, the NAS tries to communicate with other RADIUS servers in active state. If no other servers are in active state at the time, the NAS considers the authentication or accounting attempt a failure.

To set the maximum number of RADIUS request transmission attempts:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>radius scheme radius-scheme-name</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>retry retry-times</td>
<td>The default setting is 3.</td>
</tr>
</tbody>
</table>
Setting the status of RADIUS servers

To control the RADIUS servers with which the device communicates when the current servers are no longer available, set the status of RADIUS servers to blocked or active. You can specify one primary RADIUS server and multiple secondary RADIUS servers. The secondary servers act as the backup of the primary server.

When the RADIUS server load sharing feature is enabled, the device distributes the workload over all servers without considering the primary and secondary server roles. The device checks the weight value and number of currently served users for each active server, and then determines the most appropriate server in performance to receive an AAA request.

When the RADIUS server load sharing is disabled, the device chooses servers based on the following rules:

- When the primary server is in active state, the device communicates with the primary server.
- If the primary server fails, the device performs the following operations:
  - Changes the server status to blocked.
  - Starts a quiet timer for the server.
  - Tries to communicate with a secondary server in active state that has the highest priority.
- If the secondary server is unreachable, the device performs the following operations:
  - Changes the server status to blocked.
  - Starts a quiet timer for the server.
  - Tries to communicate with the next secondary server in active state that has the highest priority.
- The search process continues until the device finds an available secondary server or has checked all secondary servers in active state. If no server is available, the device considers the authentication or accounting attempt a failure.
- When the quiet timer of a server expires or you manually set the server to the active state, the status of the server changes back to active. The device does not check the server again during the authentication or accounting process.
- When you remove a server in use, communication with the server times out. The device looks for a server in active state by first checking the primary server, and then checking secondary servers in the order they are configured.
- When the primary server and secondary servers are all in blocked state, the device tries to communicate with the primary server.
- When one or more servers are in active state, the device tries to communicate with these active servers only, even if the servers are unavailable.
- When a RADIUS server's status changes automatically, the device changes this server's status accordingly in all RADIUS schemes in which this server is specified.
- When a RADIUS server is manually set to blocked, server detection is disabled for the server, regardless of whether a test profile has been specified for the server. When the RADIUS server is set to active state, server detection is enabled for the server on which an existing test profile is specified.

By default, the device sets the status of all RADIUS servers to active. However, in some situations, you must change the status of a server. For example, if a server fails, you can change the status of the server to blocked to avoid communication attempts to the server.

To set the status of RADIUS servers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td>radius scheme radius-scheme-name</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
3. Set the RADIUS server status. | - Set the status of the primary RADIUS authentication server:
   `state primary authentication { active | block }`
- Set the status of the primary RADIUS accounting server:
  `state primary accounting { active | block }`
- Set the status of a secondary RADIUS authentication server:
  `state secondary authentication [ { host-name | ipv4-address | ipv6 ipv6-address } [ port-number ]
  vpn-instance vpn-instance-name ] * ] { active | block }`
- Set the status of a secondary RADIUS accounting server:
  `state secondary accounting [ { host-name | ipv4-address | ipv6 ipv6-address } [ port-number ]
  vpn-instance vpn-instance-name ] * ] { active | block }`
| By default, every server specified in a RADIUS scheme is in active state. The configured server status cannot be saved to any configuration file, and can only be viewed by using the `display radius scheme` command. After the device restarts, all servers are restored to the active state.

### Enabling the RADIUS server load sharing feature

**IMPORTANT:**

This feature is available in Release 1121 and later.

By default, the device communicates with RADIUS servers based on the server roles. It first attempts to communicate with the primary server, and, if the primary server is unavailable, it then searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication. In this process, the workload is always placed on the active server.

Use the RADIUS server load sharing feature to dynamically distribute the workload over multiple servers regardless of their server roles. The device forwards an AAA request to the most appropriate server of all active servers in the scheme after it compares the weight values and numbers of currently served users. Specify a weight value for each RADIUS server based on the AAA capacity of the server. A larger weight value indicates a higher AAA capacity.

In RADIUS server load sharing, once the device sends a start-accounting request to a server for a user, it forwards all subsequent accounting requests of the user to the same server. If the accounting server is unreachable, the device returns an accounting failure message rather than searching for another active accounting server.

To enable the RADIUS server load sharing feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter RADIUS scheme view.</td>
<td><code>radius scheme radius-scheme-name</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable the RADIUS server load sharing feature.</td>
<td><code>algorithm loading-share enable</code></td>
<td>By default, this feature is disabled.</td>
</tr>
</tbody>
</table>

### Specifying the source IP address for outgoing RADIUS packets

The source IP address of RADIUS packets that a NAS sends must match the IP address of the NAS configured on the RADIUS server. A RADIUS server identifies a NAS by its IP address. Upon
receiving a RADIUS packet, a RADIUS server checks whether the source IP address of the packet is the IP address of a managed NAS.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

The source address of outgoing RADIUS packets is typically the IP address of an egress interface on the NAS to communicate with the RADIUS server. However, in some situations, you must change the source IP address. For example, when VRRP is configured for stateful failover, configure the virtual IP address of the uplink VRRP group as the source IP address.

You can specify a source IP address for outgoing RADIUS packets in RADIUS scheme view or in system view.

- The IP address specified in RADIUS scheme view applies only to one RADIUS scheme.
- The IP address specified in system view applies to all RADIUS schemes whose servers are in a VPN or the public network.

Before sending a RADIUS packet, the NAS selects a source IP address in the following order:
1. The source IP address specified for the RADIUS scheme.
2. The source IP address specified in system view for the VPN or public network, depending on where the RADIUS server resides.
3. The IP address of the outbound interface specified by the route.

To specify a source IP address for all RADIUS schemes in a VPN or the public network:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>radius nas-ip { ipv4-address</td>
<td>ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]</td>
</tr>
</tbody>
</table>

To specify a source IP address for a RADIUS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>radius scheme radius-scheme-name</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>nas-ip { ipv4-address</td>
<td>ipv6 ipv6-address }</td>
</tr>
</tbody>
</table>

Setting RADIUS timers

The device uses the following types of timers to control communication with a RADIUS server:

- **Server response timeout timer (response-timeout)**—Defines the RADIUS request retransmission interval. The timer starts immediately after a RADIUS request is sent. If the device does not receive a response from the RADIUS server before the timer expires, it resends the request.
- **Server quiet timer (quiet)**—Defines the duration to keep an unreachable server in blocked state. If one server is not reachable, the device changes the server status to blocked, starts this
timer for the server, and tries to communicate with another server in active state. After the server quiet timer expires, the device changes the status of the server back to active.

- **Realtime accounting timer (realtime-accounting)**—Defines the interval at which the device sends realtime accounting packets to the RADIUS accounting server for online users.

When you set RADIUS timers, follow these guidelines:

- When you configure the maximum number of RADIUS packet transmission attempts and the RADIUS server response timeout timer, consider the number of secondary servers. If the retransmission process takes too much time, the client connection in the access module (for example, Telnet) might time out during the process.
- For client connections with a short timeout period, the initial authentication or accounting might fail, even if small packet transmission attempt limit and server response timeout period are configured. However, the next authentication or accounting attempt can succeed, because the device has set the unreachable servers to blocked, which shortens the amount of time for finding a reachable server.
- Make sure the server quiet timer is set correctly. A timer that is too short might result in frequent authentication or accounting failures. This is because the device will continue to attempt to communicate with an unreachable server that is in active state. A timer that is too long might temporarily block a reachable server that has recovered from a failure. This is because the server will remain in blocked state until the timer expires.
- A short realtime accounting interval helps improve accounting precision but requires many system resources. When there are 1000 or more users, set the interval to 15 minutes or longer.

To set RADIUS timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td>radius scheme radius-scheme-name</td>
</tr>
<tr>
<td>3.</td>
<td>Set the RADIUS server response timeout timer.</td>
<td>timer response-timeout seconds</td>
</tr>
<tr>
<td>4.</td>
<td>Set the quiet timer for the servers.</td>
<td>timer quiet minutes</td>
</tr>
<tr>
<td>5.</td>
<td>Set the realtime accounting timer.</td>
<td>timer realtime-accounting minutes</td>
</tr>
</tbody>
</table>

**Configuring the accounting-on feature**

When the accounting-on feature is enabled, the device automatically sends an accounting-on packet to the RADIUS server after a reboot. Upon receiving the accounting-on packet, the RADIUS server logs out all online users so they can log in again through the device. Without this feature, users cannot log in again after the reboot, because the RADIUS server considers them to come online.

You can configure the interval for which the device waits to resend the accounting-on packet and the maximum number of retries.

The RADIUS server must run on IMC to correctly log out users when a card reboots on the distributed device to which the users connect.

To configure the accounting-on feature for a RADIUS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td>radius scheme radius-scheme-name</td>
</tr>
</tbody>
</table>
3. Enable accounting-on.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>accounting-on enable [ interval seconds</td>
<td>send send-times ] *</td>
</tr>
</tbody>
</table>

### Configuring the IP addresses of the security policy servers

The NAS verifies the validity of received control packets and accepts only control packets from known servers. To use a security policy server that is independent of the AAA servers, configure the IP address of the security policy server on the NAS.

The security policy server is the management and control center of the HPE EAD solution. To implement all EAD functions, configure both the IP address of the security policy server and that of the IMC Platform on the NAS.

To configure the IP address of a security policy server for a scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Specify a security policy server.</td>
<td>By default, no security policy server is specified for a scheme. You can specify a maximum of eight security policy servers for a RADIUS scheme.</td>
</tr>
</tbody>
</table>

### Configuring the Login-Service attribute check method for SSH, FTP, and terminal users

The device supports the following check methods for the Login-Service attribute (RADIUS attribute 15) of SSH, FTP, and terminal users:

- **Strict**—Matches Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal services, respectively.
- **Loose**—Matches the standard Login-Service attribute value 0 for SSH, FTP, and terminal services.

An Access-Accept packet received for a user must contain the matching attribute value. Otherwise, the user cannot log in to the device.

Use the loose check method only when the server does not issue Login-Service attribute values 50, 51, and 52 for SSH, FTP, and terminal users.

To configure the Login-Service attribute check method for SSH, FTP, and terminal users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter RADIUS scheme view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the Login-Service attribute check method for SSH, FTP, and terminal users.</td>
<td>The default check method is strict.</td>
</tr>
</tbody>
</table>

### Enabling SNMP notifications for RADIUS

When SNMP notifications are enabled for RADIUS, the SNMP agent supports the following notifications generated by RADIUS:
- **RADIUS server unreachable notification**—The RADIUS server cannot be reached. RADIUS generates this notification if it cannot receive any response to an accounting or authentication request within the specified RADIUS request transmission attempts.

- **RADIUS server reachable notification**—The RADIUS server can be reached. RADIUS generates this notification for a previously blocked RADIUS server after the quiet timer expires.

- **Excessive authentication failures notification**—The number of authentication failures to the total number of authentication attempts exceeds the specified threshold.

You can configure SNMP parameters to control the output of these SNMP notifications. For more information, see *Network Management and Monitoring Configuration Guide*.

To enable SNMP notifications for RADIUS:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable SNMP notifications for RADIUS.</td>
<td>snmp-agent trap enable radius [ accounting-server-down</td>
</tr>
</tbody>
</table>

**Displaying and maintaining RADIUS**

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the RADIUS scheme configuration.</td>
<td><code>display radius scheme [radius-scheme-name]</code></td>
</tr>
<tr>
<td>Display RADIUS packet statistics.</td>
<td><code>display radius statistics</code></td>
</tr>
<tr>
<td>Clear RADIUS statistics.</td>
<td><code>reset radius statistics</code></td>
</tr>
</tbody>
</table>

**Configuring HWTACACS schemes**

**Configuration task list**

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Creating an HWTACACS scheme</td>
<td></td>
</tr>
<tr>
<td>(Required.) Specifying the HWTACACS authentication servers</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Specifying the HWTACACS authorization servers</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Specifying the HWTACACS accounting servers</td>
<td></td>
</tr>
<tr>
<td>(Required.) Specifying the shared keys for secure HWTACACS communication</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Specifying a VPN for the scheme</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Setting the username format and traffic statistics units</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Specifying the source IP address for outgoing HWTACACS packets</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Setting HWTACACS timers</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Displaying and maintaining HWTACACS</td>
<td></td>
</tr>
</tbody>
</table>
Creating an HWTACACS scheme

Create an HWTACACS scheme before performing any other HWTACACS configurations. You can configure a maximum of 16 HWTACACS schemes. An HWTACACS scheme can be used by multiple ISP domains.

To create an HWTACACS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an HWTACACS scheme and enter HWTACACS scheme view.</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
</tr>
</tbody>
</table>

Specifying the HWTACACS authentication servers

You can specify one primary authentication server and a maximum of 16 secondary authentication servers for an HWTACACS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. An HWTACACS server can function as the primary authentication server in one scheme and as the secondary authentication server in another scheme at the same time.

To specify an HWTACACS server by hostname in an MPLS VPN network, first complete one of the following tasks on the device:

- Configure hostname-to-IP address mappings for the VPN by using the ip host or ipv6 host command.
- Configure a DNS server for the VPN by using the dns server or ipv6 dns server command.

For more information about these commands, see Layer 3—IP Services Command Reference.

To specify HWTACACS authentication servers for an HWTACACS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter HWTACACS scheme view.</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify HWTACACS authentication servers.</td>
<td></td>
</tr>
</tbody>
</table>

   - Specify the primary HWTACACS authentication server:
     - primary authentication { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection | vpn-instance vpn-instance-name ] *
   - Specify a secondary HWTACACS authentication server:
     - secondary authentication { host-name | ipv4-address | ipv6 ipv6-address } [ port-number | key { cipher | simple } string | single-connection | vpn-instance vpn-instance-name ] *

Specifying the HWTACACS authorization servers

You can specify one primary authorization server and a maximum of 16 secondary authorization servers for an HWTACACS scheme. When the primary server is not available, the device searches
for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. An HWTACACS server can function as the primary authorization server of one scheme and as the secondary authorization server of another scheme at the same time.

To specify an HWTACACS server by hostname in an MPLS VPN network, first complete one of the following tasks on the device:

- Configure hostname-to-IP address mappings for the VPN by using the `ip host` or `ipv6 host` command.
- Configure a DNS server for the VPN by using the `dns server` or `ipv6 dns server` command.

For more information about these commands, see *Layer 3—IP Services Command Reference*.

To specify HWTACACS authorization servers for an HWTACACS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter HWTACACS scheme view.</td>
<td>hwtacacs scheme</td>
</tr>
<tr>
<td>3.</td>
<td>Specify HWTACACS authorization servers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Specify the primary HWTACACS authorization server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`primary authorization { host-name</td>
<td>ipv4-address</td>
</tr>
<tr>
<td></td>
<td>- Specify a secondary HWTACACS authorization server:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>`secondary authorization { host-name</td>
<td>ipv4-address</td>
</tr>
</tbody>
</table>

**Specifying the HWTACACS accounting servers**

You can specify one primary accounting server and a maximum of 16 secondary accounting servers for an HWTACACS scheme. When the primary server is not available, the device searches for the secondary servers in the order they are configured. The first secondary server in active state is used for communication.

If redundancy is not required, specify only the primary server. An HWTACACS server can function as the primary accounting server of one scheme and as the secondary accounting server of another scheme at the same time.

HWTACACS does not support accounting for FTP, SFTP, and SCP users.

To specify an HWTACACS server by hostname in an MPLS VPN network, first complete one of the following tasks on the device:

- Configure hostname-to-IP address mappings for the VPN by using the `ip host` or `ipv6 host` command.
- Configure a DNS server for the VPN by using the `dns server` or `ipv6 dns server` command.

For more information about these commands, see *Layer 3—IP Services Command Reference*. 
To specify HWTACACS accounting servers for an HWTACACS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter HWTACACS scheme view.</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
</tr>
</tbody>
</table>
| 3.   | Specify HWTACACS accounting servers. | • Specify the primary HWTACACS accounting server:  
primary accounting { host-name | ipv4-address | ipv6 ipv6-address } { port-number | key { cipher | simple } string | single-connection | vpn-instance vpn-instance-name } *  
• Specify a secondary HWTACACS accounting server:  
secondary accounting { host-name | ipv4-address | ipv6 ipv6-address } { port-number | key { cipher | simple } string | single-connection | vpn-instance vpn-instance-name } * | By default, no accounting server is specified.  
Two HWTACACS accounting servers in a scheme, primary or secondary, cannot have the same combination of hostname, IP address, port number, and VPN. |

**Specifying the shared keys for secure HWTACACS communication**

The HWTACACS client and server use the MD5 algorithm and shared keys to generate the Authenticator value for packet authentication and user password encryption. The client and server must use the same key for each type of communication.

Perform this task to configure shared keys for servers in an HWTACACS scheme. The keys take effect on all servers for which a shared key is not individually configured.

To specify a shared key for secure HWTACACS communication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter HWTACACS scheme view.</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
</tr>
</tbody>
</table>
| 3.   | Specify a shared key for secure HWTACACS authentication, authorization, or accounting communication. | key { accounting | authentication | authorization } { cipher | simple } string | By default, no shared key is specified.  
The shared key configured on the device must be the same as the shared key configured on the HWTACACS server. |

**Specifying a VPN for the scheme**

The VPN specified for an HWTACACS scheme applies to all servers in that scheme. If a VPN is also configured for an individual HWTACACS server, the VPN specified for the HWTACACS scheme does not take effect on that server.

To specify a VPN for an HWTACACS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
Setting the username format and traffic statistics units

A username is in the `userid@isp-name` format, where the `isp-name` argument represents the user's ISP domain name. By default, the ISP domain name is included in a username. If HWTACACS servers do not recognize usernames that contain ISP domain names, you can configure the device to send usernames without domain names to the servers.

If two or more ISP domains use the same HWTACACS scheme, configure the HWTACACS scheme to keep the ISP domain name in usernames for domain identification.

The device reports online user traffic statistics in accounting packets. The traffic measurement units are configurable, but they must be the same as the traffic measurement units configured on the HWTACACS accounting servers.

To set the username format and traffic statistics units for an HWTACACS scheme:

### Specifying the source IP address for outgoing HWTACACS packets

The source IP address of HWTACACS packets that a NAS sends must match the IP address of the NAS configured on the HWTACACS server. An HWTACACS server identifies a NAS by IP address. When the HWTACACS server receives a packet, it checks whether the source IP address of the packet is the IP address of a managed NAS.

- If the source IP address of the packet is the IP address of a managed NAS, the server processes the packet.
- If the source IP address of the packet is not the IP address of a managed NAS, the server drops the packet.

To communicate with the HWTACACS server, the source address of outgoing HWTACACS packets is typically the IP address of an egress interface on the NAS. However, in some situations, you must change the source IP address. For example, when VRRP is configured for stateful failover, configure the virtual IP address of the uplink VRRP group as the source IP address.

You can specify the source IP address for outgoing HWTACACS packets in HWTACACS scheme view or in system view.

- The IP address specified in HWTACACS scheme view applies to one HWTACACS scheme.
- The IP address specified in system view applies to all HWTACACS schemes whose servers are in a VPN or the public network.
Before sending an HWTACACS packet, the NAS selects a source IP address in the following order:

1. The source IP address specified for the HWTACACS scheme.
2. The source IP address specified in system view for the VPN or public network, depending on where the HWTACACS server resides.
3. The IP address of the outbound interface specified by the route.

To specify a source IP address for all HWTACACS schemes of a VPN or the public network:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>hwtacacs nas-ip { ipv4-address</td>
<td>ipv6</td>
</tr>
</tbody>
</table>

To specify a source IP address for an HWTACACS scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>hwtacacs scheme hwtacacs-scheme-name</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>nas-ip { ipv4-address</td>
<td>ipv6 ipv6-address }</td>
</tr>
</tbody>
</table>

Setting HWTACACS timers

The device uses the following timers to control communication with an HWTACACS server:

- **Server response timeout timer (response-timeout)**—Defines the HWTACACS server response timeout timer. The device starts this timer immediately after an HWTACACS authentication, authorization, or accounting request is sent. If the device does not receive a response from the server within the timer, it sets the server to blocked. Then, the device sends the request to another HWTACACS server.

- **Realtime accounting timer (realtime-accounting)**—Defines the interval at which the device sends realtime accounting packets to the HWTACACS accounting server for online users.

- **Server quiet timer (quiet)**—Defines the duration to keep an unreachable server in blocked state. If a server is not reachable, the device changes the server status to blocked, starts this timer for the server, and tries to communicate with another server in active state. After the server quiet timer expires, the device changes the status of the server back to active.

The server quiet timer setting affects the status of HWTACACS servers. If the scheme includes one primary HWTACACS server and multiple secondary HWTACACS servers, the device communicates with the HWTACACS servers based on the following rules:

- When the primary server is in active state, the device communicates with the primary server.
- If the primary server fails, the device performs the following operations:
  - Changes the server status to blocked.
  - Starts a quiet timer for the server.
  - Tries to communicate with a secondary server in active state that has the highest priority.
- If the secondary server is unreachable, the device performs the following operations:
Changes the server status to blocked.
- Starts a quiet timer for the server.
- Tries to communicate with the next secondary server in active state that has the highest priority.

- The search process continues until the device finds an available secondary server or has checked all secondary servers in active state. If no server is available, the device considers the authentication, authorization, or accounting attempt a failure.
- When the quiet timer of a server expires, the status of the server changes back to active. The device does not check the server again during the authentication, authorization, or accounting process.
- When you remove a server in use, communication with the server times out. The device looks for a server in active state by first checking the primary server, and then checking secondary servers in the order they are configured.
- When the primary server and secondary servers are all in blocked state, the device tries to communicate with the primary server.
- When one or more servers are in active state, the device tries to communicate with these active servers only, even if they are unavailable.
- When an HWTACACS server’s status changes automatically, the device changes this server’s status accordingly in all HWTACACS schemes in which this server is specified.

To set HWTACACS timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter HWTACACS scheme view.</td>
<td>hwtacacs scheme hwtacacs-schema-name</td>
</tr>
<tr>
<td>3.</td>
<td>Set the HWTACACS server response timeout timer.</td>
<td>timer response-timeout seconds</td>
</tr>
<tr>
<td>4.</td>
<td>Set the realtime accounting interval.</td>
<td>timer realtime-accounting minutes</td>
</tr>
<tr>
<td>5.</td>
<td>Set the server quiet timer.</td>
<td>timer quiet minutes</td>
</tr>
</tbody>
</table>

Displaying and maintaining HWTACACS

Execute **display** commands in any view and **reset** commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the configuration or server statistics of HWTACACS schemes.</td>
<td>display hwtacacs scheme [ hwtacacs-schema-name [ statistics ] ]</td>
</tr>
<tr>
<td>Clear HWTACACS statistics.</td>
<td>reset hwtacacs statistics { accounting</td>
</tr>
</tbody>
</table>
Configuring LDAP schemes

Configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring an LDAP server:</td>
</tr>
<tr>
<td>• (Required.) Creating an LDAP server</td>
</tr>
<tr>
<td>• (Required.) Configuring the IP address of the LDAP server</td>
</tr>
<tr>
<td>• (Optional.) Specifying the LDAP version</td>
</tr>
<tr>
<td>• (Optional.) Setting the LDAP server timeout period</td>
</tr>
<tr>
<td>• (Required.) Configuring administrator attributes</td>
</tr>
<tr>
<td>• (Required.) Configuring LDAP user attributes</td>
</tr>
<tr>
<td>(Required.) Creating an LDAP scheme</td>
</tr>
<tr>
<td>(Required.) Specifying the LDAP authentication server</td>
</tr>
<tr>
<td>(Optional.) Displaying and maintaining LDAP</td>
</tr>
</tbody>
</table>

Creating an LDAP server

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an LDAP server and enter LDAP server view.</td>
<td>ldap server server-name</td>
</tr>
</tbody>
</table>

Configuring the IP address of the LDAP server

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter LDAP server view.</td>
<td>ldap server server-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the IP address of the LDAP server.</td>
<td>{ ip ip-address</td>
</tr>
</tbody>
</table>

Specifying the LDAP version

Specify the LDAP version on the NAS. The device supports LDAPv2 and LDAPv3. The LDAP version specified on the device must be consistent with the version specified on the LDAP server.

To specify the LDAP version:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter LDAP server view.</td>
<td>ldap server server-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the LDAP version.</td>
<td>protocol-version { v2</td>
</tr>
</tbody>
</table>
Setting the LDAP server timeout period

If the device sends a bind or search request to an LDAP server without receiving the server’s response within the server timeout period, the authentication or authorization request times out. Then, the device tries the backup authentication or authorization method. If no backup method is configured in the ISP domain, the device considers the authentication or authorization attempt a failure.

To set the LDAP server timeout period:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter LDAP server view.</td>
<td>ldap server server-name</td>
</tr>
<tr>
<td>3.</td>
<td>Set the LDAP server timeout period.</td>
<td>server-timeout time-interval</td>
</tr>
</tbody>
</table>

Configuring administrator attributes

To configure the administrator DN and password for binding with the LDAP server during LDAP authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter LDAP server view.</td>
<td>ldap server server-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the administrator DN.</td>
<td>login-dn dn-string</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the administrator password.</td>
<td>login-password { cipher</td>
</tr>
</tbody>
</table>

Configuring LDAP user attributes

To authenticate a user, an LDAP client must complete the following operations:

1. Establish a connection to the LDAP server.
2. Obtain the user DN from the LDAP server.
3. Use the user DN and the user password to bind with the LDAP server.

LDAP provides a DN search mechanism for obtaining the user DN. According to the mechanism, an LDAP client sends search requests to the server based on the search policy determined by the LDAP user attributes of the LDAP client.

The LDAP user attributes include:
- Search base DN.
- Search scope.
- Username attribute.
- Username format.
- User object class.

If the LDAP server contains many directory levels, a user DN search starting from the root directory can take a long time. To improve efficiency, you can change the start point by specifying the search base DN.
To configure LDAP user attributes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter LDAP server view.</td>
<td>ldap server server-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the user search base DN.</td>
<td>search-base-dn base-dn</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Specify the user search scope.</td>
<td>search-scope { all-level</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Specify the username attribute.</td>
<td>user-parameters user-name-attribute { name-attribute</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Specify the username format.</td>
<td>user-parameters user-name-format { with-domain without-domain }</td>
</tr>
<tr>
<td>7.</td>
<td>(Optional.) Specify the user object class.</td>
<td>user-parameters user-object-class object-class-name</td>
</tr>
</tbody>
</table>

Creating an LDAP scheme

You can configure a maximum of 16 LDAP schemes. An LDAP scheme can be used by multiple ISP domains.

To create an LDAP scheme:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an LDAP scheme and enter LDAP scheme view.</td>
<td>ldap ldap-scheme-name scheme ldap-scheme-name</td>
</tr>
</tbody>
</table>

Specifying the LDAP authentication server

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter LDAP scheme view.</td>
<td>ldap scheme ldap-scheme-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the LDAP authentication server.</td>
<td>authentication-server server-name</td>
</tr>
</tbody>
</table>

Displaying and maintaining LDAP

Execute display commands in any view.
## Configuring AAA methods for ISP domains

You configure AAA methods for an ISP domain by specifying configured AAA schemes in ISP domain view. Each ISP domain has a set of system-defined AAA methods, which are local authentication, local authorization, and local accounting. If you do not configure any AAA methods for an ISP domain, the device uses the system-defined AAA methods for users in the domain.

### Configuration prerequisites

To use local authentication for users in an ISP domain, configure local user accounts on the device first. See "Configuring local user attributes."

To use remote authentication, authorization, and accounting, create the required RADIUS, HWTACACS, or LDAP schemes. For more information about the scheme configuration, see "Configuring RADIUS schemes," "Configuring HWTACACS schemes," and "Configuring LDAP schemes."

### Creating an ISP domain

In a networking scenario with multiple ISPs, the device can connect to users of different ISPs. These users can have different user attributes, such as different username and password structures, different service types, and different rights. To manage users of different ISPs, configure ISP domains, and configure AAA methods and domain attributes for each ISP domain as needed.

The device supports a maximum of 16 ISP domains, including the system-defined ISP domain `system`. You can specify one of the ISP domains as the default domain. You can modify the settings of the ISP domain `system`, but you cannot delete the domain.

On the device, each user belongs to an ISP domain. If a user does not provide an ISP domain name at login, the device considers the user belongs to the default ISP domain.

The device chooses an authentication domain for each user in the following order:

1. The authentication domain specified for the access module.
2. The ISP domain in the username.
3. The default ISP domain of the device.

If the chosen domain does not exist on the device, the device searches for the ISP domain that accommodates users that are assigned to nonexistent domains. If no such ISP domain is configured, user authentication fails.

An ISP domain cannot be deleted when it is the default ISP domain. Before you use the `undo domain` command, change the domain to a non-default ISP domain by using the `undo domain default enable` command.

To create an ISP domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Create an ISP domain and enter ISP domain view.</td>
<td><code>domain isp-name</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Specify the default ISP domain.</td>
<td>domain default enable &lt;isp-name&gt;</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Specify an ISP domain to accommodate users that are assigned to nonexistent domains.</td>
<td>domain if-unknown &lt;isp-domain-name&gt;</td>
</tr>
</tbody>
</table>

### Configuring ISP domain attributes

In an ISP domain, you can configure the following attributes:

- **Domain status**—By placing the ISP domain in active or blocked state, you allow or deny network service requests from users in the domain.

- **Default authorization user profile**—When a user passes authentication, it typically obtains an authorization user profile from the local or remote server. If the user does not obtain any user profile from the server, the device authorizes the default user profile of the ISP domain to the user. The device will restrict the user behavior based on the profile.

An ISP domain attribute applies to all users in the domain.

To configure ISP domain attributes:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ISP domain view.</td>
<td>domain &lt;isp-name&gt;</td>
</tr>
<tr>
<td>3.</td>
<td>Place the ISP domain in active or blocked state.</td>
<td>state { active</td>
</tr>
<tr>
<td>4.</td>
<td>Specify an authorization user profile for authenticated users in the ISP domain.</td>
<td>authorization-attribute user-profile &lt;profile-name&gt;</td>
</tr>
</tbody>
</table>

### Configuring authentication methods for an ISP domain

**Configuration prerequisites**

Before configuring authentication methods, complete the following tasks:

1. Determine the access type or service type to be configured. With AAA, you can configure an authentication method for each access type and service type.

2. Determine whether to configure the default authentication method for all access types or service types. The default authentication method applies to all access users. However, the method has a lower priority than the authentication method that is specified for an access type or service type.

**Configuration guidelines**

When configuring authentication methods, follow these guidelines:
• If a RADIUS scheme is used for authentication but not for authorization, AAA accepts only the authentication result from the RADIUS server. The Access-Accept message from the RADIUS server also includes the authorization information, but the device ignores the information.

• If an HWTACACS scheme is specified, the device uses the entered username for role authentication. If a RADIUS scheme is specified, the device uses the username $enabn$ on the RADIUS server for role authentication. The variable n represents a user role level. For more information about user role authentication, see Fundamentals Configuration Guide.

**Configuration procedure**

To configure authentication methods for an ISP domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ISP domain view.</td>
<td>domain isp-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the default authentication method for all types of users.</td>
<td>authentication default { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme radius-scheme-name ] [ local ] [ none ]</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the authentication method for LAN users.</td>
<td>authentication lan-access { ldap-scheme ldap-scheme-name [ local ] [ none ]</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the authentication method for login users.</td>
<td>authentication login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme radius-scheme-name ] [ local ] [ none ]</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the authentication method for portal users.</td>
<td>authentication portal { ldap-scheme ldap-scheme-name [ local ] [ none ]</td>
</tr>
<tr>
<td>7.</td>
<td>Specify the authentication method for obtaining a temporary user role.</td>
<td>authentication super { hwtacacs-scheme hwtacacs-scheme-name</td>
</tr>
</tbody>
</table>

**Configuring authorization methods for an ISP domain**

**Configuration prerequisites**

Before configuring authorization methods, complete the following tasks:

1. Determine the access type or service type to be configured. With AAA, you can configure an authorization scheme for each access type and service type.
2. Determine whether to configure the default authorization method for all access types or service types. The default authorization method applies to all access users. However, the method has a lower priority than the authorization method that is specified for an access type or service type.

Configuration guidelines

When configuring authorization methods, follow these guidelines:

- The device supports HWTACACS authorization but not LDAP authorization.
- To use a RADIUS scheme as the authorization method, specify the same RADIUS scheme that is configured as the authentication method for the ISP domain. If an invalid RADIUS scheme is specified as the authorization method, RADIUS authentication and authorization fail.

Configuration procedure

To configure authorization methods for an ISP domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ISP domain view.</td>
<td>domain isp-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the default authorization method for all types of users.</td>
<td>authorization default { hwtacacs-scheme hwtacacs-scheme-name [ radius-schema radius-schema-name ] [ local ] [ none ]</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the command authorization method.</td>
<td>authorization command { hwtacacs-scheme hwtacacs-scheme-name [ local ] [ none ]</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the authorization method for LAN users.</td>
<td>authorization lan-access { local [ none ]</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the authorization method for login users.</td>
<td>authorization login { hwtacacs-scheme hwtacacs-scheme-name [ radius-schema radius-schema-name ] [ local ] [ none ]</td>
</tr>
<tr>
<td>7.</td>
<td>Specify the authorization method for portal users.</td>
<td>authorization portal { local [ none ]</td>
</tr>
</tbody>
</table>
Configuring accounting methods for an ISP domain

Configuration prerequisites

Before configuring accounting methods, complete the following tasks:

1. Determine the access type or service type to be configured. With AAA, you can configure an accounting method for each access type and service type.
2. Determine whether to configure the default accounting method for all access types or service types. The default accounting method applies to all access users. However, the method has a lower priority than the accounting method that is specified for an access type or service type.

Configuration guidelines

When configuring accounting methods, follow these guidelines:

- FTP, SFTP, and SCP users do not support accounting.
- Local accounting does not provide statistics for charging. It only counts and controls the number of concurrent users who use the same local user account. The threshold is configured by using the `access-limit` command.

Configuration procedure

To configure accounting methods for an ISP domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter ISP domain view.</td>
<td>domain isp-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the default accounting method for all types of users.</td>
<td>accounting default { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme radius-scheme-name ] [ local ] [ none ]</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the command accounting method.</td>
<td>accounting command hwtacacs-scheme hwtacacs-scheme-name</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the accounting method for LAN users.</td>
<td>accounting lan-access { local [ none ]</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the accounting method for login users.</td>
<td>accounting login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme radius-scheme-name ] [ local ] [ none ]</td>
</tr>
<tr>
<td>7.</td>
<td>Specify the accounting method for portal users.</td>
<td>accounting portal { local [ none ]</td>
</tr>
</tbody>
</table>
Enabling the session-control feature

A RADIUS server running on IMC can use session-control packets to inform disconnect or dynamic authorization change requests. This task enables the device to receive RADIUS session-control packets on UDP port 1812.

To enable the session-control feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the session-control feature.</td>
<td>radius session-control enable</td>
</tr>
</tbody>
</table>

Setting the maximum number of concurrent login users

Perform this task to set the maximum number of concurrent users who can log on to the device through a specific protocol, regardless of their authentication methods. The authentication methods include no authentication, local authentication, and remote authentication.

To set the maximum number of concurrent login users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Set the maximum number of concurrent login users. | • In non-FIPS mode: aaa session-limit { ftp | http | https | ssh | telnet } max-sessions  
• In FIPS mode: aaa session-limit { https | ssh } max-sessions | By default, the maximum number of concurrent login users is 32 for each user type. |

Configuring a NAS-ID profile

By default, the device sends its device name in the NAS-Identifier attribute of all RADIUS requests. A NAS-ID profile enables you to send different NAS-Identifier attribute strings in RADIUS requests from different VLANs. The strings can be organization names, service names, or any user categorization criteria, depending on the administrative requirements.

For example, map the NAS-ID companyA to all VLANs of company A. The device will send companyA in the NAS-Identifier attribute for the RADIUS server to identify requests from any Company A users.

You can apply a NAS-ID profile to portal- or port security-enabled interfaces. For more information, see "Configuring portal authentication" and "Configuring port security."

A NAS-ID can be bound with more than one VLAN, but a VLAN can be bound with only one NAS-ID.

To configure a NAS-ID profile:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a NAS-ID profile and enter NAS-ID profile view.</td>
<td>aaa nas-id profile profile-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a NAS-ID and VLAN binding in the profile.</td>
<td>nas-id nas-identifier bind vlan vlan-id</td>
</tr>
</tbody>
</table>

### Displaying and maintaining AAA

Execute **display** commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the configuration of ISP domains.</td>
<td>display domain [ isp-name ]</td>
</tr>
</tbody>
</table>

### AAA configuration examples

#### AAA for SSH users by an HWTACACS server

**Network requirements**

As shown in Figure 11, configure the switch to meet the following requirements:
- Use the HWTACACS server for SSH user authentication, authorization, and accounting.
- Assign the default user role **network-operator** to SSH users after they pass authentication.
- Exclude domain names from the usernames sent to the HWTACACS server.
- Use **expert** as the shared keys for secure HWTACACS communication.

**Figure 11 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. Configure the HWTACACS server:
   # Set the shared keys for secure communication with the switch to **expert**. (Details not shown.)
   # Add user account **hello** for the SSH user and specify the password. (Details not shown.)
2. Configure the switch:
   # Configure IP addresses for interfaces. (Details not shown.)
# Create an HWTACACS scheme.
<Switch> system-view
[Switch] hwtacacs scheme hwtac

# Specify the primary authentication server.
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49

# Specify the primary authorization server.
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49

# Specify the primary accounting server.
[Switch-hwtacacs-hwtac] primary accounting 10.1.1.1 49

# Set the shared keys for secure HWTACACS communication to expert in plain text.
[Switch-hwtacacs-hwtac] key authentication simple expert
[Switch-hwtacacs-hwtac] key authorization simple expert
[Switch-hwtacacs-hwtac] key accounting simple expert

# Exclude domain names from the usernames sent to the HWTACACS server.
[Switch-hwtacacs-hwtac] user-name-format without-domain

# Create ISP domain bbb and configure the domain to use the HWTACACS scheme for authentication, authorization, and accounting of login users.
[Switch-isp-bbb] authentication login hwtacacs-scheme hwtac
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting login hwtacacs-scheme hwtac

# Create local RSA and DSA key pairs.
[Switch] public-key local create rsa
[Switch] public-key local create dsa

# Enable the SSH service.
[Switch] ssh server enable

# Enable scheme authentication for user lines VTY 0 through VTY 63.
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme

# Enable the default user role feature to assign authenticated SSH users the default user role network-operator.
[Switch] role default-role enable

Verifying the configuration

# Initiate an SSH connection to the switch, and enter the username hello@bbb and the password. The user logs in to the switch. (Details not shown.)

# Verify that the user can use the commands permitted by the network-operator user role. (Details not shown.)

Local authentication, HWTACACS authorization, and RADIUS accounting for SSH users

Network requirements

As shown in Figure 12, configure the switch to meet the following requirements:

- Perform local authentication for SSH servers.
Use the HWTACACS server and RADIUS server for SSH user authorization and accounting, respectively.

Exclude domain names from the usernames sent to the servers.

Assign the default user role network-operator to SSH users after they pass authentication.

Configure an account with the username hello for the SSH user. Configure the shared keys for secure communication with the HWTACACS server and RADIUS server to expert.

**Figure 12 Network diagram**

![Network Diagram](image)

**Configuration procedure**

1. Configure the HWTACACS server. (Details not shown.)
2. Configure the RADIUS server. (Details not shown.)
3. Configure the switch:
   
   # Configure IP addresses for interfaces. (Details not shown.)
   
   # Create local RSA and DSA key pairs.
   
   ```
   <Switch> system-view
   [Switch] public-key local create rsa
   [Switch] public-key local create dsa
   ```
   
   # Enable the SSH service.
   
   ```
   [Switch] ssh server enable
   ```
   
   # Enable scheme authentication for user lines VTY 0 through VTY 63.
   
   ```
   [Switch] line vty 0 63
   [Switch-line-vty0-63] authentication-mode scheme
   [Switch-line-vty0-63] quit
   ```
   
   # Configure an HWTACACS scheme.
   
   ```
   [Switch] hwtacacs scheme hwtac
   [Switch-hwtacacs-hwtac] primary authorization 10.1.1.2 49
   [Switch-hwtacacs-hwtac] key authorization simple expert
   [Switch-hwtacacs-hwtac] user-name-format without-domain
   [Switch-hwtacacs-hwtac] quit
   ```
   
   # Configure a RADIUS scheme.
   
   ```
   [Switch] radius scheme rd
   [Switch-radius-rd] primary accounting 10.1.1.1 1813
   [Switch-radius-rd] key accounting simple expert
   [Switch-radius-rd] user-name-format without-domain
   [Switch-radius-rd] quit
   ```
   
   # Create a device management user.
[Switch] local-user hello class manage

# Assign the SSH service for the local user.
[Switch-luser-manage-hello] service-type ssh

# Set a password for the local user to 123456TESTplat&! in plain text. In FIPS mode, you must set the password in interactive mode.
[Switch-luser-manage-hello] password simple 123456TESTplat&!

[Switch-luser-manage-hello] quit

# Create ISP domain bbb and configure the login users to use local authentication, HWTACACS authorization, and RADIUS accounting.
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting login radius-scheme rd
[Switch-isp-bbb] quit

# Enable the default user role feature to assign authenticated SSH users the default user role network-operator.
[Switch] role default-role enable

Verifying the configuration

# Initiate an SSH connection to the switch, and enter the username hello@bbb and the correct password. The user logs in to the switch. (Details not shown.)

# Verify that the user can use the commands permitted by the network-operator user role. (Details not shown.)

Authentication and authorization for SSH users by a RADIUS server

Network requirements

As shown in Figure 13, configure the switch to meet the following requirements:

- Use the RADIUS server for SSH user authentication and authorization.
- Include domain names in the usernames sent to the RADIUS server.
- Assign the default user role network-operator to SSH users after they pass authentication.

The RADIUS server runs on IMC. Add an account with the username hello@bbb on the RADIUS server.

The RADIUS server and the switch use expert as the shared key for secure RADIUS communication. The ports for authentication and accounting are 1812 and 1813, respectively.
Figure 13 Network diagram

Configuration procedure

1. Configure the RADIUS server on IMC 5.0:

   NOTE:
   This example assumes that the RADIUS server runs on IMC PLAT 5.0 (E0101) and IMC UAM 5.0 (E0101).

   # Add the switch to the IMC Platform as an access device.

   Log in to IMC, click the Service tab, and select User Access Manager > Access Device Management > Access Device from the navigation tree. Then, click Add to configure an access device as follows:

   a. Set the shared key for secure RADIUS communication to expert.
   b. Set the ports for authentication and accounting to 1812 and 1813, respectively.
   c. Select the service type Device Management Service.
   d. Select the access device type HP.
   e. Select the access device from the device list or manually add the access device (with the IP address 10.1.1.2).
   f. Leave the default settings for other parameters and click OK.

   The IP address of the access device specified here must be the same as the source IP address of the RADIUS packets sent from the switch. The source IP address is chosen in the following order on the switch:

   o IP address specified by the nas-ip command.
   o IP address specified by the radius nas-ip command.
   o IP address of the outbound interface (the default).
# Add an account for device management.

Click the **User** tab, and select **Access User View > Device Mgmt User** from the navigation tree. Then, click **Add** to configure a device management account as follows:

a. Enter the account name **hello@bbb** and specify the password.

b. Select the service type **SSH**.

c. Specify 10.1.1.0 to 10.1.1.255 as the IP address range of the hosts to be managed.

d. Click **OK**.

**NOTE:**
The IP address range must contain the IP address of the switch.
2. Configure the switch:

# Configure the IP address of VLAN-interface 2, through which the SSH user accesses the switch.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

# Configure the IP address of VLAN-interface 3, through which the switch communicates with the server.

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
```

# Create local RSA and DSA key pairs.

```
[Switch] public-key local create rsa
[Switch] public-key local create dsa
```

# Enable the SSH service.

```
[Switch] ssh server enable
```

# Enable scheme authentication for user lines VTY 0 through VTY 63.

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

# Enable the default user role feature to assign authenticated SSH users the default user role network-operator.

```
[Switch] role default-role enable
```
# Create a RADIUS scheme.
[Switch] radius scheme rad

# Specify the primary authentication server.
[Switch-radius-rad] primary authentication 10.1.1.1 1812

# Set the shared key for secure communication with the server to `expert` in plain text.
[Switch-radius-rad] key authentication simple expert

# Include domain names in the usernames sent to the RADIUS server.
[Switch-radius-rad] user-name-format with-domain
[Switch-radius-rad] quit

# Create ISP domain `bbb` and configure authentication, authorization, and accounting methods for login users.
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login none
[Switch-isp-bbb] quit

Verifying the configuration

# Initiate an SSH connection to the switch, and enter the username `hello@bbb` and the correct password. The user logs in to the switch. (Details not shown.)

# Verify that the user can use the commands permitted by the network-operator user role. (Details not shown.)

Authentication for SSH users by an LDAP server

Network requirements

As shown in Figure 16, an LDAP server is located at 10.1.1.1/24 and uses the domain name `ldap.com`.

Configure the switch to meet the following requirements:

- Use the LDAP server to authenticate SSH users.
- Assign the default user role `network-operator` to SSH users after they pass authentication.

On the LDAP server, set the administrator password to `admin!123456`, add user `aaa`, and set the user password to `ldap!123456`.

Figure 16 Network diagram

Configuration procedure

1. Configure the LDAP server:
NOTE:
This example assumes that the LDAP server runs Microsoft Windows 2003 Server Active Directory.

# Add a user named aaa and set the password to ldap!123456.


b. Double-click Active Directory Users and Computers.

   The Active Directory Users and Computers window is displayed.

c. From the navigation tree, click Users under the ldap.com node.

d. Select Action > New > User from the menu to display the dialog box for adding a user.

e. Enter the logon name aaa and click Next.

   Figure 17 Adding user aaa

f. In the dialog box, enter the password ldap!123456, select options as needed, and click Next.
Figure 18 Setting the user password

- Click OK.

# Add user aaa to group Users.

- From the navigation tree, click Users under the ldap.com node.

- In the right pane, right-click the user aaa and select Properties.

- In the dialog box, click the Member Of tab and click Add.
In the Select Groups dialog box, enter Users in the Enter the object names to select field, and click OK.

User aaa is added to group Users.

Set the administrator password to admin!123456.

a. In the right pane, right-click the user Administrator and select Set Password.
b. In the dialog box, enter the administrator password. (Details not shown.)

2. Configure the switch:
# Configure the IP address of VLAN-interface 2, through which the SSH user accesses the switch.
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 24
[Switch-Vlan-interface2] quit

# Configure the IP address of VLAN-interface 3, through which the switch communicates with the server.
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 24
[Switch-Vlan-interface3] quit

# Create local RSA and DSA key pairs.
[Switch] public-key local create rsa
[Switch] public-key local create dsa

# Enable the SSH service.
[Switch] ssh server enable

# Enable scheme authentication for user lines VTY 0 through VTY 63.
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit

# Enable the default user role feature to assign authenticated SSH users the default user role network-operator.
[Switch] role default-role enable

# Configure an LDAP server.
[Switch] ldap server ldap1

# Specify the IP address of the LDAP authentication server.
[Switch-ldap-server-ldap1] ip 10.1.1.1

# Specify the administrator DN.
[Switch-ldap-server-ldap1] login-dn cn=administrator,cn=users,dc=ldap,dc=com

# Specify the administrator password.
[Switch-ldap-server-ldap1] login-password simple admin!123456

# Configure the base DN for user search.
[Switch-ldap-server-ldap1] search-base-dn dc=ldap,dc=com
[Switch-ldap-server-ldap1] quit

# Create an LDAP scheme.
[Switch] ldap scheme ldap-shm1

# Specify the LDAP authentication server.
[Switch-ldap-ldap-shm1] authentication-server ldap1
[Switch-ldap-ldap-shm1] quit

# Create ISP domain bbb and configure authentication, authorization, and accounting methods for login users.
[Switch] domain bbb
[Switch-isp-bbb] authentication login ldap-scheme ldap-shm1
[Switch-isp-bbb] authorization login none
[Switch-isp-bbb] accounting login none
[Switch-isp-bbb] quit
Verifying the configuration

# Initiate an SSH connection to the switch, and enter the username aaa@bbb and password ldap!123456. The user logs in to the switch. (Details not shown.)

# Verify that the user can use the commands permitted by the network-operator user role. (Details not shown.)

Troubleshooting RADIUS

RADIUS authentication failure

Symptom
User authentication always fails.

Analysis
Possible reasons include:
- A communication failure exists between the NAS and the RADIUS server.
- The username is not in the userid@isp-name format, or the ISP domain is not correctly configured on the NAS.
- The user is not configured on the RADIUS server.
- The password entered by the user is incorrect.
- The RADIUS server and the NAS are configured with different shared keys.

Solution
To resolve the problem:
1. Verify the following items:
   - The NAS and the RADIUS server can ping each other.
   - The username is in the userid@isp-name format and the ISP domain is correctly configured on the NAS.
   - The user is configured on the RADIUS server.
   - The correct password is entered.
   - The same shared key is configured on both the RADIUS server and the NAS.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

RADIUS packet delivery failure

Symptom
RADIUS packets cannot reach the RADIUS server.

Analysis
Possible reasons include:
- A communication failure exists between the NAS and the RADIUS server.
- The NAS is not configured with the IP address of the RADIUS server.
- The authentication and accounting UDP ports configured on the NAS are incorrect.
- The RADIUS server’s authentication and accounting port numbers are being used by other applications.
Solution
To resolve the problem:
1. Verify the following items:
   o The link between the NAS and the RADIUS server works well at both the physical and data link layers.
   o The IP address of the RADIUS server is correctly configured on the NAS.
   o The authentication and accounting UDP port numbers configured on the NAS are the same as those of the RADIUS server.
   o The RADIUS server's authentication and accounting port numbers are available.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

RADIUS accounting error

Symptom
A user is authenticated and authorized, but accounting for the user is not normal.

Analysis
The accounting server configuration on the NAS is not correct. Possible reasons include:
   • The accounting port number configured on the NAS is incorrect.
   • The accounting server IP address configured on the NAS is incorrect. For example, the NAS is configured to use a single server to provide authentication, authorization, and accounting services, but in fact the services are provided by different servers.

Solution
To resolve the problem:
1. Verify the following items:
   o The accounting port number is correctly configured.
   o The accounting server IP address is correctly configured on the NAS.
2. If the problem persists, contact Hewlett Packard Enterprise Support.

Troubleshooting HWTACACS
Similar to RADIUS troubleshooting. See "Troubleshooting RADIUS."

Troubleshooting LDAP

LDAP authentication failure

Symptom
User authentication fails.

Analysis
Possible reasons include:
   • A communication failure exists between the NAS and the LDAP server.
   • The LDAP server IP address or port number configured on the NAS is not correct.
   • The username is not in the userid@isp-name format, or the ISP domain is not correctly configured on the NAS.
• The user is not configured on the LDAP server.
• The password entered by the user is incorrect.
• The administrator DN or password is not configured.
• Some user attributes (for example, the username attribute) configured on the NAS are not consistent with those configured on the server.
• No user search base DN is specified for the LDAP scheme.

Solution
To resolve the problem:
1. Verify the following items:
   o The NAS and the LDAP server can ping each other.
   o The IP address and port number of the LDAP server configured on the NAS match those of the server.
   o The username is in the correct format and the ISP domain for the user authentication is correctly configured on the NAS.
   o The user is configured on the LDAP server.
   o The correct password is entered.
   o The administrator DN and the administrator password are correctly configured.
   o The user attributes (for example, the username attribute) configured on the NAS are consistent with those configured on the LDAP server.
   o The user search base DN for authentication is specified.
2. If the problem persists, contact Hewlett Packard Enterprise Support.
802.1X overview

802.1X is a port-based network access control protocol initially proposed for securing WLANs. The protocol has also been widely used on Ethernet networks for access control.

802.1X controls network access by authenticating the devices connected to 802.1X-enabled LAN ports.

802.1X architecture

802.1X operates in the client/server model. As shown in Figure 21, 802.1X authentication includes the following entities:

- **Client (supplicant)**—A user terminal seeking access to the LAN. The terminal must have 802.1X software to authenticate to the access device.
- **Access device (authenticator)**—Authenticates the client to control access to the LAN. In a typical 802.1X environment, the access device uses an authentication server to perform authentication.
- **Authentication server**—Provides authentication services for the access device. The authentication server first authenticates 802.1X clients by using the data sent from the access device. Then, the server returns the authentication results to the access device to make access decisions. The authentication server is typically a RADIUS server. In a small LAN, you can use the access device as the authentication server.

Figure 21 802.1X architecture

Controlled/uncontrolled port and port authorization status

802.1X defines two logical ports for the network access port: controlled port and uncontrolled port. Any packet arriving at the network access port is visible to both logical ports.

- **Uncontrolled port**—Is always open to receive and transmit authentication packets.
- **Controlled port**—Filters packets depending on the port's state.
  - **Authorized state**—The controlled port is in authorized state when the client has passed authentication. The port allows traffic to pass through.
  - **Unauthorized state**—The port is in unauthorized state when the client has failed authentication. The port controls traffic by using one of the following methods:
    - Performs bidirectional traffic control to deny traffic to and from the client.
    - Performs unidirectional traffic control to deny traffic from the client. The HPE devices support only unidirectional traffic control.
802.1X-related protocols

802.1X uses the Extensible Authentication Protocol (EAP) to transport authentication information for the client, the access device, and the authentication server. EAP is an authentication framework that uses the client/server model. The framework supports a variety of authentication methods, including MD5-Challenge, EAP-Transport Layer Security (EAP-TLS), and Protected EAP (PEAP).

802.1X defines EAP over LAN (EAPOL) for passing EAP packets between the client and the access device over a wired or wireless LAN. Between the access device and the authentication server, 802.1X delivers authentication information by using one of the following methods:

- Encapsulates EAP packets in RADIUS by using EAP over RADIUS (EAPOR), as described in "EAP relay."
- Extracts authentication information from the EAP packets and encapsulates the information in standard RADIUS packets, as described in "EAP termination."

Packet formats

EAP packet format

Figure 23 shows the EAP packet format.

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Code**—Type of the EAP packet. Options include Request (1), Response (2), Success (3), or Failure (4).
- **Identifier**—Used for matching Responses with Requests.
- **Length**—Length (in bytes) of the EAP packet. The EAP packet length is the sum of the Code, Identifier, Length, and Data fields.
• **Data**—Content of the EAP packet. This field appears only in a Request or Response EAP packet. The Data field contains the request type (or the response type) and the type data. Type 1 (Identify) and type 4 (MD5-challenge) are two examples for the type field.

**EAPOL packet format**

Figure 24 shows the EAPOL packet format.

![EAPOL packet format](image)

- **PAE Ethernet type**—Protocol type. It takes the value 0x888E for EAPOL.
- **Protocol version**—The EAPOL protocol version used by the EAPOL packet sender.
- **Type**—Type of the EAPOL packet. Table 4 lists the types of EAPOL packets supported by Hewlett Packard Enterprise implementation of 802.1X.

<table>
<thead>
<tr>
<th>Value</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>EAP-Packet</td>
<td>The client and the access device use EAP-Packets to transport authentication information.</td>
</tr>
<tr>
<td>0x01</td>
<td>EAPOL-Start</td>
<td>The client sends an EAPOL-Start message to initiate 802.1X authentication to the access device.</td>
</tr>
<tr>
<td>0x02</td>
<td>EAPOL-Logoff</td>
<td>The client sends an EAPOL-Logoff message to tell the access device that the client is logging off.</td>
</tr>
</tbody>
</table>

- **Length**—Data length in bytes, or length of the Packet body. If packet type is EAPOL-Start or EAPOL-Logoff, this field is set to 0, and no Packet body field follows.
- **Packet body**—Content of the packet. When the EAPOL packet type is EAP-Packet, the Packet body field contains an EAP packet.

**EAP over RADIUS**

RADIUS adds two attributes, EAP-Message and Message-Authenticator, for supporting EAP authentication. For the RADIUS packet format, see "Configuring AAA."

**EAP-Message**

RADIUS encapsulates EAP packets in the EAP-Message attribute, as shown in Figure 25. The Type field takes 79, and the Value field can be up to 253 bytes. If an EAP packet is longer than 253 bytes, RADIUS encapsulates it in multiple EAP-Message attributes.
Figure 25 EAP-Message attribute format

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>15</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type=79</td>
<td>Length</td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>EAP packets</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Message-Authenticator

RADIUS includes the Message-Authenticator attribute in all packets that have an EAP-Message attribute to check their integrity. The packet receiver drops the packet if the calculated packet integrity checksum is different from the Message-Authenticator attribute value. The Message-Authenticator prevents EAP authentication packets from being tampered with during EAP authentication.

Figure 26 Message-Authenticator attribute format

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>18 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type=80</td>
<td>Length</td>
<td>Value</td>
<td></td>
</tr>
</tbody>
</table>

802.1X authentication initiation

Both the 802.1X client and the access device can initiate 802.1X authentication.

802.1X client as the initiator

The client sends an EAPOL-Start packet to the access device to initiate 802.1X authentication. The destination MAC address of the packet is the IEEE 802.1X specified multicast address 01-80-C2-00-00-03 or the broadcast MAC address. If any intermediate device between the client and the authentication server does not support the multicast address, you must use an 802.1X client that can send broadcast EAPOL-Start packets. For example, you can use the HPE iNode 802.1X client.

Access device as the initiator

The access device initiates authentication, if a client cannot send EAPOL-Start packets. One example is the 802.1X client available with Windows XP.

The access device supports the following modes:

- **Multicast trigger mode**—The access device multicasts Identity EAP-Request packets to initiate 802.1X authentication at the identity request interval.

- **Unicast trigger mode**—Upon receiving a frame from an unknown MAC address, the access device sends an Identity EAP-Request packet out of the receiving port to the MAC address. The device retransmits the packet if no response has been received within the identity request timeout interval. This process continues until the maximum number of request attempts set by using the `dot1x retry` command is reached.

The username request timeout timer sets both the identity request interval for the multicast trigger and the identity request timeout interval for the unicast trigger.
802.1X authentication procedures

802.1X authentication has two methods: EAP relay and EAP termination. You choose either mode depending on support of the RADIUS server for EAP packets and EAP authentication methods.

- **EAP relay mode.**

  EAP relay is defined in IEEE 802.1X. In this mode, the network device uses EAPOR packets to send authentication information to the RADIUS server, as shown in Figure 27.

  **Figure 27 EAP relay**

  ![EAP relay diagram](image)

  In EAP relay mode, the client must use the same authentication method as the RADIUS server. On the access device, you only need to use the `dot1x authentication-method eap` command to enable EAP relay.

- **EAP termination mode.**

  As shown in Figure 28, the access device performs the following operations in EAP termination mode:

  a. Terminates the EAP packets received from the client.
  b. Encapsulates the client authentication information in standard RADIUS packets.
  c. Uses PAP or CHAP to authenticate to the RADIUS server.

  **Figure 28 EAP termination**

  ![EAP termination diagram](image)

Comparing EAP relay and EAP termination

<table>
<thead>
<tr>
<th>Packet method</th>
<th>exchange</th>
<th>Benefits</th>
<th>Limitations</th>
</tr>
</thead>
</table>
| EAP relay     |          | - Supports various EAP authentication methods.  
- The configuration and processing are simple on the access device.  | The RADIUS server must support the EAP-Message and Message-Authenticator attributes, and the EAP authentication method used by the client. |
| EAP termination | Works with any RADIUS server that supports PAP or CHAP authentication. | Supports only the following EAP authentication methods:  
- MD5-Challenge EAP authentication.  
- The username and password EAP authentication initiated by an HPE iNode 802.1X client. |
### EAP relay

Figure 29 shows the basic 802.1X authentication procedure in EAP relay mode, assuming that EAP-MD5 is used.

**Figure 29 802.1X authentication procedure in EAP relay mode**

The following steps describe the 802.1X authentication procedure:

1. When a user launches the 802.1X client and enters a registered username and password, the 802.1X client sends an EAPOL-Start packet to the access device.
2. The access device responds with an Identity EAP-Request packet to ask for the client username.
3. In response to the Identity EAP-Request packet, the client sends the username in an Identity EAP-Response packet to the access device.
4. The access device relays the Identity EAP-Response packet in a RADIUS Access-Request packet to the authentication server.
5. The authentication server uses the identity information in the RADIUS Access-Request to search its user database. If a matching entry is found, the server uses a randomly generated
challenge (EAP-Request/MD5 challenge) to encrypt the password in the entry. Then, the server sends the challenge in a RADIUS Access-Challenge packet to the access device.

6. The access device transmits the EAP-Request/MD5 Challenge packet to the client.

7. The client uses the received challenge to encrypt the password, and sends the encrypted password in an EAP-Response/MD5 Challenge packet to the access device.

8. The access device relays the EAP-Response/MD5 Challenge packet in a RADIUS Access-Request packet to the authentication server.

9. The authentication server compares the received encrypted password with the encrypted password it generated at step 5. If the two passwords are identical, the server considers the client valid and sends a RADIUS Access-Accept packet to the access device.

10. Upon receiving the RADIUS Access-Accept packet, the access device performs the following operations:
    a. Sends an EAP-Success packet to the client.
    b. Sets the controlled port in authorized state.

The client can access the network.

11. After the client comes online, the access device periodically sends handshake requests to check whether the client is still online. By default, if two consecutive handshake attempts fail, the device logs off the client.

12. Upon receiving a handshake request, the client returns a response. If the client fails to return a response after a number of consecutive handshake attempts (two by default), the access device logs off the client. This handshake mechanism enables timely release of the network resources used by 802.1X users who have abnormally gone offline.

13. The client can also send an EAPOL-Logoff packet to ask the access device for a logoff.

14. In response to the EAPOL-Logoff packet, the access device changes the status of the controlled port from authorized to unauthorized. Then, the access device sends an EAP-Failure packet to the client.

**EAP termination**

Figure 30 shows the basic 802.1X authentication procedure in EAP termination mode, assuming that CHAP authentication is used.
In EAP termination mode, the access device rather than the authentication server generates an MD5 challenge for password encryption. The access device then sends the MD5 challenge together with the username and encrypted password in a standard RADIUS packet to the RADIUS server.
Configuring 802.1X

This chapter describes how to configure 802.1X on an HPE device. You can also configure the port security feature to perform 802.1X. Port security combines and extends 802.1X and MAC authentication. It applies to a network that requires different authentication methods for different users on a port. For more information about the port security feature, see "Configuring port security."

Access control methods

HPE implements port-based access control as defined in the 802.1X protocol, and extends the protocol to support MAC-based access control.

- **Port-based access control**—Once an 802.1X user passes authentication on a port, any subsequent user can access the network through the port without authentication. When the authenticated user logs off, all other users are logged off.

- **MAC-based access control**—Each user is separately authenticated on a port. When a user logs off, no other online users are affected.

802.1X VLAN manipulation

Authorization VLAN

The device uses the authorization VLAN to control the access of an 802.1X user to authorized network resources.

Supported VLAN types and forms

Support for VLAN types and forms depends on the authorization type.

- **Local VLAN authorization.**
  
  The authorization VLAN of an 802.1X user is specified in user view or user group view in the form of VLAN ID on the device. The port through which the user accesses the device is assigned to the VLAN as an untagged member. Tagged VLAN assignment is not supported. For more information about local user configuration, see "Configuring AAA."

- **Remote VLAN authorization.**
  
  The authorization VLAN information of an 802.1X user is assigned by a remote server. The device resolves the VLAN information and selects a VLAN as the authorization VLAN for the user. The port through which the user accesses the device can be assigned to the VLAN as a tagged or untagged member.

  The access device can resolve server-assigned VLANs in the following forms:

  - VLAN ID.
  - VLAN name.
    
    The VLAN name represents the VLAN description on the access device.

  - Combination of VLAN IDs and VLAN names.
    
    In the string, some VLANs are represented by their IDs, and some VLANs are represented by their names.

  - VLAN group name.
    
    For more information about VLAN groups, see *Layer 2—LAN Switching Configuration Guide*.

  - VLAN ID with suffix.
The suffix can be `t` or `u`, which indicates whether the ports assigned to the VLAN are tagged members. For example, `2u` indicates that the ports assigned to VLAN 2 are untagged members.

**NOTE:**
The access device converts VLAN names and VLAN group name into VLAN IDs before VLAN assignment.

**Unsupported VLAN types**
Do not specify the following types of VLANs for VLAN authorization. The access device does not assign these VLANs to 802.1X users.
- VLANs that have not been created.
- Dynamically-learned VLANs.
- Reserved VLANs.
- Super VLANs.
- Private VLANs.

**VLAN selection and assignment**
If the server assigns a group of VLANs, the access device selects and assigns a VLAN according to the VLAN ID format. **Table 5** describes the VLAN selection and assignment rules for a group of authorization VLANs.

**Table 5 VLAN selection and assignment for a group of authorization VLANs**

<table>
<thead>
<tr>
<th>Types of authorized VLANs</th>
<th>VLAN selection and assignment rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>• VLANs by IDs</td>
<td>The device selects a VLAN as the authorization VLAN for a user, depending on whether the port has other online users:</td>
</tr>
<tr>
<td>• VLANs by names</td>
<td>• If the port does not have other online users, the device selects the VLAN with the lowest ID from the group of VLANs.</td>
</tr>
<tr>
<td>• VLAN group name</td>
<td>• If the port has other online users, the device selects the VLAN by using the following process:</td>
</tr>
<tr>
<td></td>
<td>a. The device selects the VLAN that has the fewest number of online users.</td>
</tr>
<tr>
<td></td>
<td>b. If two VLANs have the same number of online 802.1X users, the device selects the VLAN with the lower ID.</td>
</tr>
<tr>
<td></td>
<td>The device follows the rules in <strong>Table 6</strong> to handle VLAN assignment.</td>
</tr>
</tbody>
</table>

**VLAN IDs with suffixes**
1. The device selects the leftmost VLAN ID without a suffix, or the leftmost VLAN ID suffixed by `u` as an untagged VLAN, whichever is more leftmost.
2. The device assigns the untagged VLAN to the port as the PVID, and it assigns the remaining as tagged VLANs. If no untagged VLAN is assigned, the PVID of the port does not change. The port permits traffic from these tagged and untagged VLANs to pass through.

For example, the authentication server sends the string `1u 2t 3` to the access device for a user. The device assigns VLAN 1 as an untagged VLAN and other VLANs as tagged VLANs. VLAN 1 becomes the PVID.

**NOTE:**
Assign VLAN IDs with suffixes only to hybrid or trunk ports that perform port-based access control.

**Table 6** describes how the access device handles VLANs (except for the VLANs specified with suffixes) on an 802.1X-enabled port.
Table 6 VLAN manipulation

<table>
<thead>
<tr>
<th>Port access control method</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-based</td>
<td>The device assigns the port to the first authenticated user's authorization VLAN. All subsequent 802.1X users can access the VLAN without authentication. If the port is assigned to the authorization VLAN as an untagged member, the authorization VLAN becomes the PVID. If the port is assigned to the authorization VLAN as a tagged member, the PVID of the port does not change.</td>
</tr>
</tbody>
</table>
| MAC-based                  | • For a hybrid port with MAC-based VLAN enabled, the device maps the MAC address of each user to its own authorization VLAN. The PVID of the port does not change.  
• For an access, trunk, or MAC-based VLAN-disabled hybrid port:  
  o If the port is assigned to the authorization VLAN as an untagged member, the device assigns the port to the first authenticated user's authorization VLAN. The authorization VLAN becomes the PVID. To ensure successful authentication of subsequent users, authorize the same VLAN to all 802.1X users on the port. If a different VLAN is authorized to a subsequent user, the user cannot pass the authentication.  
  o If the port is assigned to the authorization VLAN as a tagged member, the PVID of the port does not change. The device maps the MAC address of each user to its own authorization VLAN. |

**IMPORTANT:**
- An 802.1X-enabled access port can be assigned to an authorization VLAN only as an untagged member.
- 802.1X support for tagged VLAN assignment is available in Release 1121 and later.

A hybrid port is always assigned to a VLAN as an untagged member. After the assignment, do not reconfigure the port as a tagged member in the VLAN.

On a port enabled with periodic online user reauthentication, the MAC-based VLAN feature does not take effect on a user who has been online before this feature was enabled. The access device creates a MAC-to-VLAN mapping for the user when the following requirements are met:
- The user passes reauthentication.
- The authorization VLAN for the user is changed.

For more information about VLAN configuration and MAC-based VLANs, see *Layer 2—LAN Switching Configuration Guide*.

**Guest VLAN**

The 802.1X guest VLAN on a port accommodates users who have not performed 802.1X authentication. Users in the guest VLAN can access a limited set of network resources, such as a software server, to download antivirus software and system patches. Once a user in the guest VLAN passes 802.1X authentication, it is removed from the guest VLAN and can access authorized network resources.

The access device handles VLANs on an 802.1X-enabled port based on its 802.1X access control method:
- On a port that performs port-based access control:
**Authentication status** | **VLAN manipulation**
--- | ---
A user has not passed 802.1X authentication. | The device assigns the 802.1X guest VLAN to the port as the PVID. All 802.1X users on this port can access only resources in the guest VLAN. If no 802.1X guest VLAN is configured, the access device does not perform any VLAN operation.

A user in the 802.1X guest VLAN fails 802.1X authentication. | If an 802.1X Auth-Fail VLAN (see "Auth-Fail VLAN") is available, the device assigns the Auth-Fail VLAN to the port as the PVID. All users on this port can access only resources in the Auth-Fail VLAN. If no Auth-Fail VLAN is configured, the PVID on the port is still the 802.1X guest VLAN. All users on the port are in the guest VLAN.

A user in the 802.1X guest VLAN passes 802.1X authentication. | • The device assigns the authorization VLAN of the user to the port as the PVID, and it removes the port from the 802.1X guest VLAN. After the user logs off, the initial PVID of the port is restored.
• If the authentication server does not authorize a VLAN, the initial PVID applies. The user and all subsequent 802.1X users are assigned to the initial port VLAN. After the user logs off, the port VLAN remains unchanged.

NOTE: The initial PVID of an 802.1X-enabled port refers to the PVID used by the port before the port is assigned to any 802.1X VLANs.

On a port that performs MAC-based access control:

<table>
<thead>
<tr>
<th>Authentication status</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user has not passed 802.1X authentication.</td>
<td>The device creates a mapping between the MAC address of the user and the 802.1X guest VLAN. The user can access only resources in the guest VLAN.</td>
</tr>
</tbody>
</table>

A user in the 802.1X guest VLAN fails 802.1X authentication. | If an 802.1X Auth-Fail VLAN is available, the device remaps the MAC address of the user to the Auth-Fail VLAN. The user can access only resources in the Auth-Fail VLAN. If no 802.1X Auth-Fail VLAN is configured, the user is still in the 802.1X guest VLAN. |

A user in the 802.1X guest VLAN passes 802.1X authentication. | The device remaps the MAC address of the user to the authorization VLAN. If the authentication server does not authorize a VLAN, the device remaps the MAC address of the user to the initial PVID on the port. |

For the 802.1X guest VLAN feature to take effect on a port that performs MAC-based access control, make sure the following requirements are met:
- The port is a hybrid port.
- MAC-based VLAN is enabled on the port.

The network device assigns a hybrid port to an 802.1X guest VLAN as an untagged member. For more information about VLAN configuration and MAC-based VLANs, see *Layer 2—LAN Switching Configuration Guide*.

**Auth-Fail VLAN**

The 802.1X Auth-Fail VLAN on a port accommodates users who have failed 802.1X authentication because of the failure to comply with the organization security strategy. For example, the VLAN accommodates users who have entered a wrong password. Users in the Auth-Fail VLAN can access a limited set of network resources, such as a software server, to download antivirus software and system patches.

The Auth-Fail VLAN does not accommodate 802.1X users who have failed authentication for authentication timeouts or network connection problems.
The access device handles VLANs on an 802.1X-enabled port based on its 802.1X access control method.

- On a port that performs port-based access control:

<table>
<thead>
<tr>
<th>Authentication status</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user fails 802.1X authentication.</td>
<td>The device assigns the Auth-Fail VLAN to the port as the PVID. All 802.1X users on this port can access only resources in the Auth-Fail VLAN.</td>
</tr>
<tr>
<td>A user in the 802.1X Auth-Fail VLAN fails 802.1X authentication because of any other reason except for unreachable servers.</td>
<td>The Auth-Fail VLAN is still the PVID on the port, and all 802.1X users on this port are in this VLAN.</td>
</tr>
</tbody>
</table>
| A user passes 802.1X authentication. | • The device assigns the authorization VLAN of the user to the port as the PVID, and it removes the port from the Auth-Fail VLAN. After the user logs off, the guest VLAN is assigned to the port as the PVID. If no guest VLAN is configured, the initial PVID of the port is restored.  
• If the authentication server does not authorize a VLAN, the device remaps the MAC address of the user to the initial PVID on the port. |

- On a port that performs MAC-based access control:

<table>
<thead>
<tr>
<th>Authentication status</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user fails 802.1X authentication.</td>
<td>The device maps the MAC address of the user to the 802.1X Auth-Fail VLAN. The user can access only resources in the Auth-Fail VLAN.</td>
</tr>
<tr>
<td>A user in the 802.1X Auth-Fail VLAN fails 802.1X authentication because of any other reason except for unreachable servers.</td>
<td>The user is still in the Auth-Fail VLAN.</td>
</tr>
<tr>
<td>A user in the 802.1X Auth-Fail VLAN passes 802.1X authentication.</td>
<td>The device remaps the MAC address of the user to the authorization VLAN. If the authentication server does not authorize a VLAN, the device remaps the MAC address of the user to the initial PVID on the port.</td>
</tr>
</tbody>
</table>

For the 802.1X Auth-Fail VLAN feature to take effect on a port that performs MAC-based access control, make sure the following requirements are met:
- The port is a hybrid port.
- MAC-based VLAN is enabled on the port.

The access device assigns a hybrid port to an 802.1X Auth-Fail VLAN as an untagged member. For more information about VLAN configuration and MAC-based VLANs, see *Layer 2—LAN Switching Configuration Guide*. Support for the MAC-based VLAN feature depends on the device model.

**Critical VLAN**

The 802.1X critical VLAN on a port accommodates 802.1X users who have failed authentication because none of the RADIUS servers in their ISP domain is reachable. Users in the critical VLAN can access a limited set of network resources depending on the configuration.

The critical VLAN feature takes effect when 802.1X authentication is performed only through RADIUS servers. If an 802.1X user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN. For more information about RADIUS configuration, see "Configuring AAA."
The access device handles VLANs on an 802.1X-enabled port based on its 802.1X access control method.

- On a port that performs port-based access control:

<table>
<thead>
<tr>
<th>Authentication status</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.</td>
<td>The device assigns the critical VLAN to the port as the PVID. The 802.1X user and all subsequent 802.1X users on this port can access only resources in the 802.1X critical VLAN.</td>
</tr>
<tr>
<td>A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable.</td>
<td>The critical VLAN is still the PVID of the port, and all 802.1X users on this port are in this VLAN.</td>
</tr>
<tr>
<td>A user in the 802.1X critical VLAN fails authentication for any other reasons except for unreachable servers.</td>
<td>If an 802.1X Auth-Fail VLAN is configured, the PVID of the port changes to the Auth-Fail VLAN ID. All 802.1X users on this port are moved to the Auth-Fail VLAN. If no 802.1X Auth-Fail VLAN is configured, the initial PVID of the port is restored.</td>
</tr>
</tbody>
</table>
| A user in the 802.1X critical VLAN passes 802.1X authentication. | - The device assigns the authorization VLAN of the user to the port as the PVID, and it removes the port from the 802.1X critical VLAN. After the user logs off, the guest VLAN ID changes to the PVID. If no 802.1X guest VLAN is configured, the initial PVID of the port is restored.  
- If the authentication server (either the local access device or a RADIUS server) does not authorize a VLAN, the initial PVID of the port applies. The user and all subsequent 802.1X users are assigned to this port VLAN. After the user logs off, the PVID remains unchanged. |
| A user in the 802.1X guest VLAN fails authentication because all the RADIUS servers are unreachable. | The device assigns the 802.1X critical VLAN to the port as the PVID, and all 802.1X users on this port are in this VLAN.                                  |
| A user in the 802.1X Auth-Fail VLAN fails authentication because all the RADIUS servers are unreachable. | The PVID of the port remains unchanged. All 802.1X users on this port can access only resources in the 802.1X Auth-Fail VLAN.                          |
| A user who has passed authentication fails reauthentication because all the RADIUS servers are unreachable, and the user is logged out of the device. | The device assigns the 802.1X critical VLAN to the port as the PVID.                                                                                   |

- On a port that performs MAC-based access control:

<table>
<thead>
<tr>
<th>Authentication status</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.</td>
<td>The device maps the MAC address of the user to the 802.1X critical VLAN. The user can access only resources in the 802.1X critical VLAN.</td>
</tr>
<tr>
<td>A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable.</td>
<td>The user is still in the critical VLAN.</td>
</tr>
</tbody>
</table>
| A user in the 802.1X critical VLAN fails 802.1X authentication for any other reasons except for unreachable servers. | If an 802.1X Auth-Fail VLAN is configured, the device remaps the MAC address of the user to the Auth-Fail VLAN ID.  
If no 802.1X Auth-Fail VLAN has been configured, the device remaps the MAC address of the user to the initial |
A user in the 802.1X critical VLAN passes 802.1X authentication. The device remaps the MAC address of the user to the authorization VLAN.

If the authentication server (either the local access device or a RADIUS server) does not authorize a VLAN to the user, the device remaps the MAC address of the user to the initial PVID on the port.

A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable. The device remaps the MAC address of the user to the initial PVID on the port.

A user in the 802.1X Critical VLAN fails authentication because all the RADIUS servers are unreachable. The user remains in the 802.1X Critical VLAN.

For the 802.1X Critical VLAN feature to take effect on a port that performs MAC-based access control, make sure the following requirements are met:

- The port is a hybrid port.
- MAC-based VLAN is enabled on the port.

The network device assigns a hybrid port to an 802.1X Critical VLAN as an untagged member.

For more information about VLAN configuration and MAC-based VLANs, see Layer 2—LAN Switching Configuration Guide.

When a reachable RADIUS server is detected, the device performs the following operations:

- If MAC-based access control is used, the device removes 802.1X users from the critical VLAN. The port sends unicast Identity EAP/Request packets to these users to trigger authentication.
- If port-based access control is used, the device removes the port from the critical VLAN. The port sends a multicast Identity EAP/Request to all 802.1X users on the port to trigger authentication.

Critical voice VLAN

**IMPORTANT:**
This feature is available in Release 1121 and later.

The 802.1X critical voice VLAN on a port accommodates 802.1X voice users who have failed authentication because none of the RADIUS servers in their ISP domain is reachable.

The critical voice VLAN feature takes effect when 802.1X authentication is performed only through RADIUS servers. If an 802.1X voice user fails local authentication after RADIUS authentication, the voice user is not assigned to the critical voice VLAN. For more information about the authentication methods, see "Configuring AAA."

When a reachable RADIUS server is detected, the device performs the following operations:

- If port-based access control is used, the device removes the port from the critical voice VLAN. The port sends a multicast EAP-Request/Identity packet to all 802.1X voice users on the port to trigger authentication.
- If MAC-based access control is used, the device removes 802.1X voice users from the critical voice VLAN. The port sends a unicast EAP-Request/Identity packet to each 802.1X voice user that was assigned to the critical voice VLAN to trigger authentication.
Using 802.1X authentication with other features

ACL assignment

You can specify an ACL for an 802.1X user to control its access to network resources. After the user passes 802.1X authentication, the authentication server assigns the ACL to the access port to filter traffic from this user. The authentication server can be the local access device or a RADIUS server. In either case, you must configure the ACL on the access device.

To ensure a successful ACL assignment, make sure the ACL does not contain rules that match source MAC addresses.

To change the access control criteria for the user, you can use one of the following methods:

- Modify ACL rules on the access device.
- Specify another authorization ACL on the authentication server.

For more information about ACLs, see "ACL and QoS Configuration Guide".

User profile assignment

You can specify a user profile for an 802.1X user to control the user's access to network resources. After the user passes 802.1X authentication, the authentication server assigns the user profile to the user for filtering traffic. The authentication server can be the local access device or a RADIUS server. In either case, you must configure the user profile on the access device.

To change the user's access permissions, you can use one of the following methods:

- Modify the user profile configuration on the access device.
- Specify another user profile for the user on the authentication server.

For more information about user profiles, see "Configuring user profiles."

EAD assistant

Endpoint Admission Defense (EAD) is an HPE integrated endpoint access control solution to improve the threat defensive capability of a network. The solution enables the security client, security policy server, access device, and third-party server to operate together. If a terminal device seeks to access an EAD network, it must have an EAD client, which performs 802.1X authentication.

EAD assistant enables the access device to redirect a user who is seeking to access the network to download and install an EAD client. This feature eliminates the administrative task to deploy EAD clients.

The EAD assistant feature is implemented by the following functionalities:

- **Free IP.**
  A free IP is a freely accessible network segment, which has a limited set of network resources such as software and DHCP servers. To ensure security strategy compliance, an unauthenticated user can access only this segment to perform operations. For example, the user can download EAD client from a software server or obtain a dynamic IP address from a DHCP server.

- **Redirect URL.**
  If an unauthenticated 802.1X user is using a Web browser to access the network, the EAD assistant feature redirects the user to a specific URL. For example, you can use this feature to redirect the user to the EAD client software download page.

The EAD assistant feature automatically creates an ACL-based EAD rule to open access to the redirect URL for each redirected user.
EAD rules are implemented by using ACL resources. When the EAD rule timer expires or the user passes authentication, the rule is removed. If users fail to download EAD client or fail to pass authentication before the timer expires, they must reconnect to the network to access the free IP.

Configuration prerequisites

Before you configure 802.1X, complete the following tasks:

- Configure an ISP domain and AAA scheme (local or RADIUS authentication) for 802.1X users.
- If RADIUS authentication is used, create user accounts on the RADIUS server.
- If local authentication is used, create local user accounts on the access device and set the service type to **lan-access**.

For more information about RADIUS client configuration, see "Configuring AAA."

802.1X configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling 802.1X</td>
</tr>
<tr>
<td>(Required.) Enabling EAP relay or EAP termination</td>
</tr>
<tr>
<td>(Optional.) Setting the port authorization state</td>
</tr>
<tr>
<td>(Optional.) Specifying an access control method</td>
</tr>
<tr>
<td>(Optional.) Setting the maximum number of concurrent 802.1X users on a port</td>
</tr>
<tr>
<td>(Optional.) Setting the maximum number of authentication request attempts</td>
</tr>
<tr>
<td>(Optional.) Setting the maximum number of 802.1X authentication attempts for MAC authenticated users</td>
</tr>
<tr>
<td>(Optional.) Setting the 802.1X authentication timeout timers</td>
</tr>
<tr>
<td>(Optional.) Configuring the online user handshake feature</td>
</tr>
<tr>
<td>(Optional.) Configuring the authentication trigger feature</td>
</tr>
<tr>
<td>(Optional.) Specifying a mandatory authentication domain on a port</td>
</tr>
<tr>
<td>(Optional.) Configuring the quiet timer</td>
</tr>
<tr>
<td>(Optional.) Enabling the periodic online user reauthentication feature</td>
</tr>
<tr>
<td>(Optional.) Configuring an 802.1X guest VLAN</td>
</tr>
<tr>
<td>(Optional.) Enabling 802.1X guest VLAN assignment delay</td>
</tr>
<tr>
<td>(Optional.) Configuring an 802.1X Auth-Fail VLAN</td>
</tr>
<tr>
<td>(Optional.) Configuring an 802.1X critical VLAN</td>
</tr>
<tr>
<td>(Optional.) Enabling the 802.1X critical voice VLAN</td>
</tr>
<tr>
<td>(Optional.) Specifying supported domain name delimiters</td>
</tr>
<tr>
<td>(Optional.) Configuring the EAD assistant feature</td>
</tr>
</tbody>
</table>

Enabling 802.1X

When you enable 802.1X, follow these guidelines:
• If the PVID is a voice VLAN, the 802.1X feature cannot take effect on the port. For more information about voice VLANs, see Layer 2—LAN Switching Configuration Guide.
• Do not enable 802.1X on a port that is in a link aggregation or service loopback group.

To enable 802.1X:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable 802.1X globally.</td>
<td>dot1x</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable 802.1X on a port.</td>
<td>dot1x</td>
</tr>
</tbody>
</table>

Enabling EAP relay or EAP termination

When configuring EAP relay or EAP termination, consider the following factors:
• Support of the RADIUS server for EAP packets.
• Authentication methods supported by the 802.1X client and the RADIUS server.

You can use both EAP termination and EAP relay in any of the following situations:
• The client is using only MD5-Challenge EAP authentication. If EAP termination is used, you must enable CHAP authentication on the access device.
• The client is an iNode 802.1X client and initiates only the username and password EAP authentication. If EAP termination is used, you can enable either PAP or CHAP authentication on the access device. However, for the purpose of security, you must use CHAP authentication on the access device.

To use EAP-TLS, PEAP, or any other EAP authentication methods, you must use EAP relay. When you make your decision, see "Comparing EAP relay and EAP termination" for help.

For more information about EAP relay and EAP termination, see "802.1X authentication procedures."

To configure EAP relay or EAP termination:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure EAP relay or EAP termination.</td>
<td>dot1x authentication-method { chap</td>
</tr>
</tbody>
</table>

NOTE:
If EAP relay mode is used, the user-name-format command configured in RADIUS scheme view does not take effect. The access device sends the authentication data from the client to the server without any modification.
Setting the port authorization state

The port authorization state determines whether the client is granted access to the network or not. You can control the authorization state of a port by using the `dot1x port-control` command and the following keywords:

- **authorized-force**—Places the port in the authorized state, enabling users on the port to access the network without authentication.
- **unauthorized-force**—Places the port in the unauthorized state, denying any access requests from users on the port.
- **auto**—Places the port initially in unauthorized state to allow only EAPOL packets to pass. After a user passes authentication, sets the port in the authorized state to allow access to the network. You can use this option in most scenarios.

To set the authorization state of a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the port authorization state.</td>
<td><code>dot1x port-control { authorized-force unauthorized-force auto }</code></td>
</tr>
</tbody>
</table>

Specifying an access control method

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Specify an access control method.</td>
<td>`dot1x port-method { macbased</td>
</tr>
</tbody>
</table>

Setting the maximum number of concurrent 802.1X users on a port

Perform this task to prevent the system resources from being overused.

To set the maximum number of concurrent 802.1X users on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the maximum number of concurrent 802.1X users on a port.</td>
<td><code>dot1x max-user user-number</code></td>
</tr>
</tbody>
</table>
Setting the maximum number of authentication request attempts

The access device retransmits an authentication request if it does not receive any responses to the request from the client within a period of time. To set the time, use the `dot1x timer tx-period tx-period-value` command or the `dot1x timer supp-timeout supp-timeout-value` command. The access device stops retransmitting the request if it has made the maximum number of request transmission attempts but still receives no response.

To set the maximum number of authentication request attempts:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the maximum number of attempts for sending an authentication request.</td>
<td><code>dot1x retry max-retry-value</code></td>
</tr>
</tbody>
</table>

Setting the maximum number of 802.1X authentication attempts for MAC authenticated users

**IMPORTANT:**
This feature is available in Release 1121 and later.

When a port uses both 802.1X authentication and MAC authentication, the device accepts 802.1X authentication requests from MAC authenticated users. If a MAC authenticated user passes 802.1X authentication, the user will come online as an 802.1X user. If the user fails 802.1X authentication, the user continues to make 802.1X authentication attempts depending on the client configuration.

Perform this task to limit the number of 802.1X authentication attempts made by a MAC authenticated user.

To set the maximum number of 802.1X authentication attempts for MAC authenticated users on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the maximum number of 802.1X authentication attempts for MAC authenticated users on the port.</td>
<td><code>dot1x after-mac-auth max-attempt max-attempts</code></td>
</tr>
</tbody>
</table>

Setting the 802.1X authentication timeout timers

The network device uses the following 802.1X authentication timeout timers:
• **Client timeout timer**—Starts when the access device sends an EAP-Request/MD5 Challenge packet to a client. If no response is received when this timer expires, the access device retransmits the request to the client.

• **Server timeout timer**—Starts when the access device sends a RADIUS Access-Request packet to the authentication server. If no response is received when this timer expires, the access device retransmits the request to the server.

In most cases, the default settings are sufficient. You can edit the timers, depending on the network conditions.

• In a low-speed network, increase the client timeout timer.

• In a network with authentication servers of different performance, adjust the server timeout timer.

To set the 802.1X authentication timeout timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the client timeout timer. dot1x timer supp-timeout supp-timeout-value</td>
</tr>
<tr>
<td>3.</td>
<td>Set the server timeout timer. dot1x timer server-timeout server-timeout-value</td>
</tr>
</tbody>
</table>

### Configuring the online user handshake feature

The online user handshake feature checks the connectivity status of online 802.1X users. The access device sends handshake requests (EAP-Request/Identity) to online users at the interval specified by the `dot1x timer handshake-period` command. If the device does not receive any EAP-Response/Identity packets from an online user after it has made the maximum handshake attempts, the device sets the user to offline state. To set the maximum handshake attempts, use the `dot1x retry` command.

Typically, the device does not reply to 802.1X clients’ EAP-Response/Identity packets with EAP-Success packets. Some 802.1X clients will go offline if they do not receive the EAP-Success packets for handshake. To avoid this problem, enable the online user handshake reply feature.

If iNode clients are deployed, you can also enable the online user handshake security feature to check authentication information in the handshake packets from clients. This feature can prevent 802.1X users who use illegal client software from bypassing iNode security check, such as dual network interface cards (NICs) detection. If a user fails the handshake security checking, the device sets the user to the offline state.

### Configuration guidelines

When you configure the online user handshake feature, follow these restrictions and guidelines:

• To use the online user handshake security feature, make sure the online user handshake feature is enabled.

• The online user handshake security feature takes effect only on the network where the iNode client and IMC server are used.

• If the network has 802.1X clients that cannot exchange handshake packets with the access device, disable the online user handshake feature. This operation prevents the 802.1X connections from being incorrectly torn down.

• Enable the online user handshake reply feature only if 802.1X clients will go offline without receiving EAP-Success packets from the device.
Configuration procedure

To configure the online user handshake feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Set the handshake timer.</td>
<td>dot1x timer handshake-period handshake-period-value</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Enable the online handshake feature.</td>
<td>dot1x handshake</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Enable the online user handshake security feature.</td>
<td>dot1x handshake secure</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Enable the 802.1X online user handshake reply feature.</td>
<td>dot1x handshake reply enable</td>
</tr>
</tbody>
</table>

Configuring the authentication trigger feature

The authentication trigger feature enables the access device to initiate 802.1X authentication when 802.1X clients cannot initiate authentication.

This feature provides the multicast trigger and unicast trigger (see 802.1X authentication initiation in "802.1X overview").

Configuration guidelines

When you configure the authentication trigger feature, follow these guidelines:
- Enable the multicast trigger on a port when the clients attached to the port cannot send EAPOL-Start packets to initiate 802.1X authentication.
- Enable the unicast trigger on a port if only a few 802.1X clients are attached to the port and these clients cannot initiate authentication.
- To avoid duplicate authentication packets, do not enable both triggers on a port.

Configuration procedure

To configure the authentication trigger feature on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Set the username request timeout timer.</td>
<td>dot1x timer tx-period tx-period-value</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type</td>
</tr>
</tbody>
</table>
### Specifying a mandatory authentication domain on a port

You can place all 802.1X users in a mandatory authentication domain for authentication, authorization, and accounting on a port. No user can use an account in any other domain to access the network through the port. The implementation of a mandatory authentication domain enhances the flexibility of 802.1X access control deployment.

To specify a mandatory authentication domain for a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Specify a mandatory 802.1X authentication domain on the port.</td>
<td>dot1x mandatory-domain domain-name</td>
<td>By default, no mandatory 802.1X authentication domain is specified.</td>
</tr>
</tbody>
</table>

### Configuring the quiet timer

The quiet timer enables the access device to wait a period of time before it can process any authentication request from a client that has failed an 802.1X authentication.

You can edit the quiet timer, depending on the network conditions.

- In a vulnerable network, set the quiet timer to a high value.
- In a high-performance network with quick authentication response, set the quiet timer to a low value.

To configure the quiet timer:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable the quiet timer.</td>
<td>dot1x quiet-period</td>
<td>By default, the timer is disabled.</td>
</tr>
<tr>
<td>3. (Optional.) Set the quiet timer.</td>
<td>dot1x timer quiet-period quiet-period-value</td>
<td>The default is 60 seconds.</td>
</tr>
</tbody>
</table>
Enabling the periodic online user reauthentication feature

Periodic online user reauthentication tracks the connection status of online users, and updates the authorization attributes assigned by the server. The attributes include the ACL, VLAN, and user profile-based QoS. The reauthentication interval is user configurable.

The server-assigned RADIUS Session-Timeout (attribute 27) and Termination-Action (attribute 29) attributes can affect the periodic online user reauthentication feature. To display the server-assigned Session-Timeout and Termination-Action attributes, use the `display dot1x connection` command (see Security Command Reference).

- If the termination action is logging off users, periodic reauthentication takes effect only when the periodic reauthentication timer is shorter than the session timeout timer. If the session timeout timer is shorter, the device logs off online authenticated users when the session timeout timer expires.
- If the termination action is reauthenticating users, the periodic online user reauthentication configuration on the device cannot take effect. The device reauthenticates online 802.1X users after the session timeout timer expires.

Support for the server configuration and assignment of session timeout timer and termination action depends on the server model.

If no server is reachable for 802.1X reauthentication, the device logs off the user or keeps it online, depending on the configuration on the device.

The VLANs assigned to an online user before and after reauthentication can be the same or different.

To enable the periodic online user reauthentication feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Set the periodic reauthentication timer.</td>
<td><code>dot1x timer reauth-period reauth-period-value</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>4.</td>
<td>Enable periodic online user reauthentication.</td>
<td><code>dot1x re-authenticate</code></td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Enable the keep-online feature for 802.1X users.</td>
<td><code>dot1x re-authenticate server-unreachable keep-online</code></td>
</tr>
</tbody>
</table>

Configuring an 802.1X guest VLAN

Configuration guidelines

When you configure an 802.1X guest VLAN, follow these guidelines:

- You can configure only one 802.1X guest VLAN on a port. The 802.1X guest VLANs on different ports can be different.
Assign different IDs to the voice VLAN, the port VLAN, and the 802.1X guest VLAN on a port. The assignment makes sure the port can correctly process incoming VLAN-tagged traffic.

When you configure multiple security features on a port, follow the guidelines in Table 7.

**Table 7 Relationships of the 802.1X guest VLAN and other security features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Relationship description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super VLAN</td>
<td>You cannot specify a VLAN as both a super VLAN and an 802.1X guest VLAN.</td>
<td>See Layer 2—LAN Switching Configuration Guide.</td>
</tr>
<tr>
<td>802.1X Auth-Fail VLAN on a port that performs MAC-based access control</td>
<td>The 802.1X Auth-Fail VLAN has a higher priority than the 802.1X guest VLAN.</td>
<td>See &quot;802.1X VLAN manipulation.&quot;</td>
</tr>
<tr>
<td>Port intrusion protection actions on a port that performs MAC-based access control</td>
<td>The 802.1X guest VLAN feature has higher priority than the block MAC action. The 802.1X guest VLAN feature has lower priority than the shutdown port action of the port intrusion protection feature.</td>
<td>See &quot;Configuring port security.&quot;</td>
</tr>
</tbody>
</table>

**Configuration prerequisites**

Before you configure an 802.1X guest VLAN, complete the following tasks:

- Create the VLAN to be specified as the 802.1X guest VLAN.
- If the 802.1X-enabled port performs MAC-based access control, perform the following operations for the port:
  - Configure the port as a hybrid port.
  - Enable MAC-based VLAN on the port. For more information about the MAC-based VLAN feature, see Layer 2—LAN Switching Configuration Guide.
  - Assign the port to the 802.1X guest VLAN as an untagged member.

**Configuration procedure**

To configure an 802.1X guest VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the 802.1X guest VLAN on the port.</td>
<td>dot1x guest-vlan guest-vlan-id</td>
</tr>
</tbody>
</table>

**Enabling 802.1X guest VLAN assignment delay**

**IMPORTANT:**

This feature is available in Release 1121 and later.

This feature delays assigning an 802.1X-enabled port to the 802.1X guest VLAN when 802.1X authentication is triggered by packets from unknown MAC addresses on the port.
This feature does not take effect if the 802.1X authentication is triggered by EAPOL-Start packets from 802.1X clients.

To use this feature, the 802.1X-enabled port must be configured with the unicast trigger feature and perform MAC-based access control.

When 802.1X authentication is triggered on a port, the device performs the following operations:

1. Sends a unicast EAP-Request/Identity packet to the MAC address that triggers the authentication.
2. Retransmits the packet if no response is received within the username request timeout interval set by using the `dot1x timer tx-period` command.
3. Assigns the port to the 802.1X guest VLAN after the maximum number of request attempts set by using the `dot1x retry` command is reached.

To enable 802.1X guest VLAN assignment delay on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enable 802.1X guest VLAN assignment delay on the port.</td>
<td><code>dot1x guest-vlan-delay</code></td>
</tr>
</tbody>
</table>

### Configuring an 802.1X Auth-Fail VLAN

#### Configuration guidelines

When you configure an 802.1X Auth-Fail VLAN, follow these restrictions and guidelines:

- Assign different IDs to the voice VLAN, the port VLAN, and the 802.1X Auth-Fail VLAN on a port. The assignment ensures that the port can correctly process VLAN-tagged incoming traffic.
- You can configure only one 802.1X Auth-Fail VLAN on a port. The 802.1X Auth-Fail VLANs on different ports can be different.
- When you configure multiple security features on a port, follow the guidelines in Table 8.

#### Table 8 Relationships of the 802.1X Auth-Fail VLAN with other features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Relationship description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super VLAN</td>
<td>You cannot specify a VLAN as both a super VLAN and an 802.1X Auth-Fail VLAN.</td>
<td>See Layer 2—LAN Switching Configuration Guide.</td>
</tr>
<tr>
<td>MAC authentication guest VLAN on a port that performs MAC-based access control</td>
<td>The 802.1X Auth-Fail VLAN has a high priority.</td>
<td>See &quot;Configuring MAC authentication.&quot;</td>
</tr>
<tr>
<td>Port intrusion protection actions on a port that performs MAC-based access control</td>
<td>The 802.1X Auth-Fail VLAN feature has higher priority than the block MAC action. The 802.1X Auth-Fail VLAN feature has lower priority than the shutdown port action of the port intrusion protection feature.</td>
<td>See &quot;Configuring port security.&quot;</td>
</tr>
</tbody>
</table>
Configuration prerequisites

Before you configure an 802.1X Auth-Fail VLAN, complete the following tasks:

- Create the VLAN to be specified as the 802.1X Auth-Fail VLAN.
- If the 802.1X-enabled port performs MAC-based access control, perform the following operations for the port:
  - Configure the port as a hybrid port.
  - Enable MAC-based VLAN on the port. For more information about the MAC-based VLAN feature, see Layer 2—LAN Switching Configuration Guide.
  - Assign the port to the Auth-Fail VLAN as an untagged member.

Configuration procedure

To configure an 802.1X Auth-Fail VLAN:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>dot1x auth-fail vlan authfail-vlan-id</td>
<td>By default, no 802.1X Auth-Fail VLAN is configured.</td>
</tr>
</tbody>
</table>

Configuring an 802.1X critical VLAN

Configuration guidelines

When you configure an 802.1X critical VLAN, follow these restrictions and guidelines:

- Assign different IDs to the voice VLAN, the PVID, and the 802.1X critical VLAN on a port. The assignment makes sure the port can correctly process VLAN-tagged incoming traffic.
- You can configure only one 802.1X critical VLAN on a port. The 802.1X critical VLANs on different ports can be different.
- You cannot specify a VLAN as both a super VLAN and an 802.1X critical VLAN. For information about super VLANs, see Layer 2—LAN Switching Configuration Guide.

Configuration prerequisites

Before you configure an 802.1X critical VLAN, complete the following tasks:

- Create the VLAN to be specified as a critical VLAN.
- If the 802.1X-enabled port performs MAC-based access control, perform the following operations for the port:
  - Configure the port as a hybrid port.
  - Enable MAC-based VLAN on the port. For more information about the MAC-based VLAN feature, see Layer 2—LAN Switching Configuration Guide.
  - Assign the port to the 802.1X critical VLAN as an untagged member.
Configuring the 802.1X critical VLAN on a port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the 802.1X critical VLAN on the port.</td>
<td>dot1x critical vlan vlan-id</td>
</tr>
</tbody>
</table>

Sending EAP-Success packets to users in the 802.1X critical VLAN

**IMPORTANT:**
This feature is available in Release 1121 and later.

Typically, the device sends EAP-Failure packets to 802.1X clients when the client users are assigned to the 802.1X critical VLAN. Some 802.1X clients, such as Windows built-in 802.1X clients, cannot respond to the EAP-Request/Identity packets of the device if they have received an EAP-Failure packet. As a result, reauthentication fails for these clients when an authentication server is reachable.

This feature enables the device to send EAP-Success packets instead of EAP-Failure packets to 802.1X clients when the client users are assigned to the 802.1X critical VLAN. This operation ensures that all 802.1X clients can perform reauthentication.

To configure the device to send an EAP-Success packet to an 802.1X client when its client user is assigned to the critical VLAN on the port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the device to send an EAP-Success packet to an 802.1X client when its client user is assigned to the critical VLAN on the port.</td>
<td>dot1x critical eapol</td>
</tr>
</tbody>
</table>

Enabling the 802.1X critical voice VLAN

**IMPORTANT:**
This feature is available in Release 1121 and later.

Configuration restrictions and guidelines

The feature does not take effect if the voice user has been in the 802.1X Auth-Fail VLAN.
Configuration prerequisites

Before you enable the 802.1X critical voice VLAN on a port, complete the following tasks:

- Enable LLDP both globally and on the port.
  The device uses LLDP to identify voice users. For information about LLDP, see Layer 2—LAN Switching Configuration Guide.
- Enable voice VLAN on the port.
  For information about voice VLANs, see Layer 2—LAN Switching Configuration Guide.

Configuration procedure

To enable the 802.1X critical voice VLAN feature on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>dot1x critical-voice-vlan</td>
<td>By default, the 802.1X critical voice VLAN feature is disabled on a port.</td>
</tr>
</tbody>
</table>

Specifying supported domain name delimiters

By default, the access device supports the at sign (@) as the delimiter. You can also configure the access device to accommodate 802.1X users who use other domain name delimiters. The configurable delimiters include the at sign (@), backslash (\), dot (.), and forward slash (/). Usernames that include domain names can use the format of username@domain-name, domain-nameusername, username.domain-name, or username/domain-name.

If an 802.1X username string contains multiple configured delimiters, the rightmost delimiter is the domain name delimiter. For example, if you configure the backslash (\), dot (.), and forward slash (/) as delimiters, the domain name delimiter for the username string 121.123/22\@abc is the backslash (\). The username is \@abc and the domain name is 121.123/22.

If a username string contains none of the delimiters, the access device authenticates the user in the mandatory or default ISP domain.

To specify a set of domain name delimiters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>dot1x domain-delimiter string</td>
<td>By default, only the at sign (@) delimiter is supported.</td>
</tr>
</tbody>
</table>

NOTE:
If you configure the access device to send usernames with domain names to the RADIUS server, make sure the domain delimiter can be recognized by the RADIUS server. For username format configuration, see the user-name-format command in Security Command Reference.
Configuring the EAD assistant feature

When you configure the EAD assistant feature, follow these restrictions and guidelines:

- You must disable MAC authentication and port security globally before you enable the EAD assistant feature.
- To make the EAD assistant feature take effect on an 802.1X-enabled port, you must set the port authorization mode to auto.
- When global MAC authentication or port security is enabled, the free IP does not take effect.
- If you use free IP, guest VLAN, and Auth-Fail VLAN features together, make sure the free IP segments are in both guest VLAN and Auth-Fail VLAN.
- To allow a user to obtain a dynamic IP address before it passes 802.1X authentication, make sure the DHCP server is on the free IP segment.
- The server that provides the redirect URL must be on the free IP accessible to unauthenticated users.
- To avoid using up ACL resources when a large number of EAD users exist, you can shorten the EAD rule timer.

To configure the EAD assistant feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable EAD assistant.</td>
<td>dot1x ead-assistant enable</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a free IP.</td>
<td>dot1x ead-assistant free-ip ip-address { mask-length</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure the redirect URL.</td>
<td>dot1x ead-assistant url url-string</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Set the EAD rule timer.</td>
<td>dot1x timer ead-timeout ead-timeout-value</td>
</tr>
</tbody>
</table>

Displaying and maintaining 802.1X

Execute the display commands in any view and reset commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display 802.1X session information, statistics, or configuration information of specified or all ports.</td>
<td>display dot1x [ sessions</td>
</tr>
<tr>
<td>Display online 802.1X user information.</td>
<td>display dot1x connection [ interface interface-type interface-number</td>
</tr>
<tr>
<td>Clear 802.1X statistics.</td>
<td>reset dot1x statistics [ interface interface-type interface-number ]</td>
</tr>
<tr>
<td>Remove users from the 802.1X guest VLAN on a port.</td>
<td>reset dot1x guest-vlan interface interface-type interface-number [ mac-address mac-address ]</td>
</tr>
</tbody>
</table>
802.1X authentication configuration examples

Basic 802.1X authentication configuration example

Network requirements

As shown in Figure 31, the access device performs 802.1X authentication for users that connect to port GigabitEthernet 1/0/1. Implement MAC-based access control on the port, so the logoff of one user does not affect other online 802.1X users.

Use RADIUS servers to perform authentication, authorization, and accounting for the 802.1X users. If RADIUS authentication fails, perform local authentication on the access device.

Configure the host at 10.1.1.1/24 as the primary authentication and accounting servers, and the host at 10.1.1.2/24 as the secondary authentication and accounting servers. Assign all users to the ISP domain bbb.

Configure the shared key as name for packets between the access device and the authentication server. Configure the shared key as money for packets between the access device and the accounting server.

Figure 31 Network diagram

Configuration procedure

1. Configure the 802.1X client. If HPE iNode is used, do not select the Carry version info option in the client configuration. (Details not shown.)

2. Configure the RADIUS servers and add user accounts for the 802.1X users. (Details not shown.)
   For information about the RADIUS commands used on the access device in this example, see Security Command Reference.

3. Assign an IP address for each interface on the access device. (Details not shown.)

4. Configure user accounts for the 802.1X users on the access device:
   # Add a local network access user with the username localuser, and password localpass in plaintext. (Make sure the username and password are the same as those configured on the RADIUS servers.)
   <Device> system-view
   [Device] local-user localuser class network
   [Device-luser-network-localuser] password simple localpass
   # Set the service type to lan-access.
   [Device-luser-network-localuser] service-type lan-access
   [Device-luser-network-localuser] quit
5. Configure a RADIUS scheme:
   # Create the RADIUS scheme radius1 and enter RADIUS scheme view.
   [Device] radius scheme radius1
   # Specify the IP addresses of the primary authentication and accounting RADIUS servers.
   [Device-radius-radius1] primary authentication 10.1.1.1
   [Device-radius-radius1] primary accounting 10.1.1.1
   # Configure the IP addresses of the secondary authentication and accounting RADIUS servers.
   [Device-radius-radius1] secondary authentication 10.1.1.2
   [Device-radius-radius1] secondary accounting 10.1.1.2
   # Specify the shared key between the access device and the authentication server.
   [Device-radius-radius1] key authentication simple name
   # Specify the shared key between the access device and the accounting server.
   [Device-radius-radius1] key accounting simple money
   # Exclude the ISP domain name from the usernames sent to the RADIUS servers.
   [Device-radius-radius1] user-name-format without-domain
   [Device-radius-radius1] quit

NOTE:
The access device must use the same username format as the RADIUS server. If the RADIUS server includes the ISP domain name in the username, so must the access device.

6. Configure the ISP domain:
   # Create the ISP domain bbb and enter ISP domain view.
   [Device] domain bbb
   # Apply the RADIUS scheme radius1 to the ISP domain, and specify local authentication as the secondary authentication method.
   [Device-isp-bbb] authentication lan-access radius-scheme radius1 local
   [Device-isp-bbb] authorization lan-access radius-scheme radius1 local
   [Device-isp-bbb] accounting lan-access radius-scheme radius1 local
   [Device-isp-bbb] quit

7. Configure 802.1X:
   # Enable 802.1X on GigabitEthernet 1/0/1.
   [Device] interface gigabitethernet 1/0/1
dot1x
   # Enable MAC-based access control on the port. By default, the port uses MAC-based access control.
   [Device-GigabitEthernet1/0/1] dot1x port-method macbased
   # Specify ISP domain bbb as the mandatory domain.
   [Device-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
   [Device-GigabitEthernet1/0/1] quit
   # Enable 802.1X globally.
   [Device] dot1x

Verifying the configuration
   # Verify the 802.1X configuration on GigabitEthernet 1/0/1.
   [Device] display dot1x interface gigabitethernet 1/0/1
   # Display the user connection information after an 802.1X user passes authentication.
   [Device] display dot1x connection
802.1X guest VLAN and authorization VLAN configuration example

Network requirements

As shown in Figure 32, use RADIUS servers to perform authentication, authorization, and accounting for 802.1X users who connect to GigabitEthernet 1/0/2. Implement port-based access control on the port.

If no user performs 802.1X authentication on GigabitEthernet 1/0/2 within a period of time, the device adds GigabitEthernet 1/0/2 to the guest VLAN, VLAN 10. The host and the update server are both in VLAN 10, and the host can access the update server and download the 802.1X client software.

After the host passes 802.1X authentication, the access device assigns the host to VLAN 5 where GigabitEthernet 1/0/3 is. The host can access the Internet.

Figure 32 Network diagram

Configuration procedure

1. Configure the 802.1X client. Make sure the 802.1X client can update its IP address after the access port is assigned to the guest VLAN or an authorization VLAN. (Details not shown.)

2. Configure the RADIUS server to provide authentication, authorization, and accounting services. Configure user accounts and authorization VLAN (VLAN 5 in this example) for the users. (Details not shown.)

3. Create VLANs, and assign ports to the VLANs on the access device.

```
<Device> system-view
[Device] vlan 1
[Device-vlan1] port gigabitethernet 1/0/2
[Device-vlan1] quit
[Device] vlan 10
```
4. Configure a RADIUS scheme on the access device:
   # Create RADIUS scheme 2000 and enter RADIUS scheme view.
   [Device] radius scheme 2000
   # Specify the server at 10.11.1.1 as the primary authentication server, and set the authentication port to 1812.
   [Device-radius-2000] primary authentication 10.11.1.1 1812
   # Specify the server at 10.11.1.1 as the primary accounting server, and set the accounting port to 1813.
   [Device-radius-2000] primary accounting 10.11.1.1 1813
   # Set the shared key to abc in plain text for secure communication between the authentication server and the device.
   [Device-radius-2000] key authentication simple abc
   # Set the shared key to abc in plain text for secure communication between the accounting server and the device.
   [Device-radius-2000] key accounting simple abc
   # Exclude the ISP domain name from the usernames sent to the RADIUS server.
   [Device-radius-2000] user-name-format without-domain
   [Device-radius-2000] quit

5. Configure an ISP domain:
   # Create ISP domain bbb and enter ISP domain view.
   [Device] domain bbb
   # Apply RADIUS scheme 2000 to the ISP domain for authentication, authorization, and accounting.
   [Device-isp-bbb] authentication lan-access radius-scheme 2000
   [Device-isp-bbb] authorization lan-access radius-scheme 2000
   [Device-isp-bbb] accounting lan-access radius-scheme 2000
   [Device-isp-bbb] quit

6. Configure 802.1X on the access device:
   # Enable 802.1X on port GigabitEthernet 1/0/2.
   [Device] interface gigabitethernet 1/0/2
   [Device-GigabitEthernet1/0/2] dot1x
   # Implement port-based access control on the port.
   [Device-GigabitEthernet1/0/2] dot1x port-method portbased
   # Set the port authorization mode to auto. By default, the port uses the auto mode.
   [Device-GigabitEthernet1/0/2] dot1x port-control auto
   # Set VLAN 10 as the 802.1X guest VLAN on port GigabitEthernet 1/0/2.
   [Device-GigabitEthernet1/0/2] dot1x guest-vlan 10
   [Device-GigabitEthernet1/0/2] quit
   # Enable 802.1X globally.
   [Device] dot1x
Verifying the configuration

# Verify the 802.1X guest VLAN configuration on GigabitEthernet 1/0/2.
[Device] display dot1x interface gigabitethernet 1/0/2

# Verify that GigabitEthernet 1/0/2 is assigned to VLAN 10 when no user passes authentication on the port.
[Device] display vlan 10

# After a user passes authentication, display information on GigabitEthernet 1/0/2. Verify that GigabitEthernet 1/0/2 is assigned to VLAN 5.
[Device] display interface gigabitethernet 1/0/2

802.1X with ACL assignment configuration example

Network requirements

As shown in Figure 33, the host that connects to GigabitEthernet 1/0/1 must pass 802.1X authentication to access the Internet.

Perform 802.1X authentication on GigabitEthernet 1/0/1. Use the RADIUS server at 10.1.1.1 as the authentication and authorization server, and the RADIUS server at 10.1.1.2 as the accounting server.

Configure ACL assignment on GigabitEthernet 1/0/1 to deny access of 802.1X users to the FTP server from 8:00 to 18:00 on weekdays.

Figure 33 Network diagram

Configuration procedure

1. Configure the 802.1X client. Make sure the client is able to update its IP address after the access port is assigned to the 802.1X guest VLAN or an authorization VLAN. (Details not shown.)

2. Configure the RADIUS servers to provide authentication, authorization, and accounting services. Add user accounts and specify the ACL (ACL 3000 in this example) for the users. (Details not shown.)

3. Assign an IP address to each interface, as shown in Figure 33. (Details not shown.)

4. Configure a RADIUS scheme:
   # Create RADIUS scheme 2000 and enter RADIUS scheme view.
   <Device> system-view
   [Device] radius-view
   # Specify the server at 10.1.1.1 as the primary authentication server, and set the authentication port to 1812.
   [Device-radius-2000] primary authentication 10.1.1.1 1812
# Specify the server at 10.1.1.2 as the primary accounting server, and set the accounting port to 1813.

```
[Device-radius-2000] primary accounting 10.1.1.2 1813
```

# Set the shared key to abc in plain text for secure communication between the authentication server and the device.

```
[Device-radius-2000] key authentication simple abc
```

# Set the shared key to abc in plain text for secure communication between the accounting server and the device.

```
[Device-radius-2000] key accounting simple abc
```

# Exclude the ISP domain name from the usernames sent to the RADIUS server.

```
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

5. Configure an ISP domain:

# Create ISP domain bbb and enter ISP domain view.

```
[Device] domain bbb
```

# Apply RADIUS scheme 2000 to the ISP domain for authentication, authorization, and accounting.

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

6. Configure a time range named ftp from 8:00 to 18:00 on weekdays.

```
[Device] time-range ftp 8:00 to 18:00 working-day
```

7. Configure ACL 3000 to deny packets destined for the FTP server at 10.0.0.1 during the specified time range.

```
[Device] acl number 3000
[Device-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp
[Device-acl-adv-3000] quit
```

8. Configure 802.1X:

# Enable 802.1X globally.

```
[Device] dot1x
```

# Enable 802.1X on GigabitEthernet 1/0/1.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] quit
```

Verifying the configuration

# Use the user account to pass authentication. (Details not shown.)

# Verify that the user cannot ping the FTP server at any time from 8:00 to 18:00 on any weekday.

```
C:\>ping 10.0.0.1
```

Pinging 10.0.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.0.1:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

The output shows that ACL 3000 is active on the user, and the user cannot access the FTP server.

802.1X with EAD assistant configuration example

Network requirements

As shown in Figure 34:

- The intranet 192.168.1.0/24 is attached to GigabitEthernet 1/0/1 of the access device.
- The hosts use DHCP to obtain IP addresses.
- A DHCP server and a Web server are deployed on the 192.168.2.0/24 subnet for users to obtain IP addresses and download client software.

Deploy an EAD solution for the intranet to meet the following requirements:

- Allow unauthenticated users and users who have failed 802.1X authentication to access 192.168.2.0/24. The users can obtain IP addresses and download software.
- If these users use a Web browser to access a network other than 192.168.2.0/24, redirect them to the Web server for 802.1X client downloading.
- Allow authenticated 802.1X users to access the network.

Figure 34 Network diagram

Configuration procedure

1. Make sure the DHCP server, the Web server, and the authentication servers have been configured correctly. (Details not shown.)
2. Configure an IP address for each interface. (Details not shown.)
3. Configure DHCP relay:
   
   ```
   # Enable DHCP.
   <Device> system-view
   [Device] dhcp enable
   # Enable the DHCP relay agent on VLAN-interface 2.
   [Device] interface vlan-interface 2
   ```
[Device-Vlan-interface2] dhcp select relay
# Specify the DHCP server 192.168.2.2 on the relay agent interface VLAN-interface 2.
[Device-Vlan-interface2] dhcp relay server-address 192.168.2.2
[Device-Vlan-interface2] quit

4. Configure a RADIUS scheme:
# Create RADIUS scheme 2000 and enter RADIUS scheme view.
[Device] radius scheme 2000
# Specify the server at 10.1.1.1 as the primary authentication server, and set the authentication port to 1812.
[Device-radius-2000] primary authentication 10.1.1.1 1812
# Specify the server at 10.1.1.2 as the primary accounting server, and set the accounting port to 1813.
[Device-radius-2000] primary accounting 10.1.1.2 1813
# Set the shared key to abc in plain text for secure communication between the authentication server and the device.
[Device-radius-2000] key authentication simple abc
# Set the shared key to abc in plain text for secure communication between the accounting server and the device.
[Device-radius-2000] key accounting simple abc
# Exclude the ISP domain name from the usernames sent to the RADIUS server.
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit

5. Configure an ISP domain:
# Create ISP domain bbb and enter ISP domain view.
[Device] domain bbb
# Apply RADIUS scheme 2000 to the ISP domain for authentication, authorization, and accounting.
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit

6. Configure 802.1X:
# Configure the free IP.
[Device] dot1x ead-assistant free-ip 192.168.2.0 24
# Configure the redirect URL for client software download.
[Device] dot1x ead-assistant url http://192.168.2.3
# Enable the EAD assistant feature.
[Device] dot1x ead-assistant enable
# Enable 802.1X globally.
[Device] dot1x
# Enable 802.1X on GigabitEthernet 1/0/1.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] quit

Verifying the configuration
# Verify the 802.1X configuration.
[Device] display dot1x

101
# Verify that you can ping an IP address on the free IP subnet from a host.

```
C:\>ping 192.168.2.3
```

Pinging 192.168.2.3 with 32 bytes of data:

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

Ping statistics for 192.168.2.3:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The output shows that you can access the free IP subnet before passing 802.1X authentication.

# Verify that you are redirected to the Web server when you enter in your Web browser an IP address not on the free IP. (Details not shown.)

## Troubleshooting 802.1X

### EAD assistant for Web browser users

**Symptom**

Unauthenticated users are not redirected to the specified redirect URL after they enter external website addresses in their Web browsers.

**Analysis**

Redirection will not happen for one of the following reasons:

- The address is in the string format. The operating system of the host regards the string as a website name and tries to resolve the string. If the resolution fails, the operating system sends an ARP request, but the target address is not in the dotted decimal notation. The redirection feature does redirect this kind of ARP request.
- The address is within a free IP segment. No redirection will take place, even if no host is present with the address.
- The redirect URL is not in a free IP segment.
- No server is using the redirect URL, or the server with the URL does not provide Web services.

**Solution**

To resolve the problem:

1. Enter a dotted decimal IP address that is not in any free IP segments.
2. Verify that the access device and the server are configured correctly.
3. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring MAC authentication

Overview

MAC authentication controls network access by authenticating source MAC addresses on a port. The feature does not require client software, and users do not have to enter a username and password for network access. The device initiates a MAC authentication process when it detects an unknown source MAC address on a MAC authentication-enabled port. If the MAC address passes authentication, the user can access authorized network resources. If the authentication fails, the device marks the MAC address as a silent MAC address, drops the packet, and starts a quiet timer. The device drops all subsequent packets from the MAC address within the quiet time. The quiet mechanism avoids repeated authentication during a short time.

NOTE:
If the MAC address that has failed authentication is a static MAC address or a MAC address that has passed any security authentication, the device does not mark the MAC address as a silent address.

User account policies

MAC authentication supports the following user account policies:

- One MAC-based user account for each user. The access device uses the source MAC addresses in packets as the usernames and passwords of users for MAC authentication. This policy is suitable for an insecure environment.
- One shared user account for all users. You specify one username and password, which are not necessarily a MAC address, for all MAC authentication users on the access device. This policy is suitable for a secure environment.

Authentication methods

You can perform MAC authentication on the access device (local authentication) or through a RADIUS server.

Local authentication:

- **MAC-based accounts**—The access device uses the source MAC address of the packet as the username and password to search the local account database for a match.
- **A shared account**—The access device uses the shared account username and password to search the local account database for a match.

RADIUS authentication:

- **MAC-based accounts**—The access device sends the source MAC address of the packet as the username and password to the RADIUS server for authentication.
- **A shared account**—The access device sends the shared account username and password to the RADIUS server for authentication.

For more information about configuring local authentication and RADIUS authentication, see "Configuring AAA."
VLAN assignment

Authorization VLAN

The device uses the authorization VLAN to control the access of a MAC authentication user to authorized network resources.

The device supports the following VLAN authorization methods:

- **Remote VLAN authorization**—The authorization VLAN information of a MAC authentication user is assigned by a remote server. The device can resolve server-assigned VLANs in the form of VLAN ID or VLAN name.
  
  The port through which the user accesses the device is assigned to the authorization VLAN as a tagged or untagged member.

- **Local VLAN authorization**—The authorization VLAN of a MAC authentication user is specified in user view or user group view in the form of VLAN ID on the device.
  
  The port through which the user accesses the device is assigned to the VLAN as an untagged member. Tagged VLAN assignment is not supported.

  For more information about local authorization VLAN configuration, see "Configuring AAA."

Table 9 describes the way the network access device handles authorization VLANs for MAC authenticated users.

<table>
<thead>
<tr>
<th>Port type</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access port</td>
<td>If the port is assigned to the authorization VLAN as an untagged member, the device assigns the port to the first authenticated user's authorization VLAN. The authorization VLAN becomes the PVID. All MAC authentication users on the port must be assigned the same authorization VLAN. If a different authorization VLAN is assigned to a subsequent user, the user cannot pass MAC authentication.</td>
</tr>
<tr>
<td>Trunk port</td>
<td></td>
</tr>
<tr>
<td>Hybrid port with MAC-based-VLAN disabled</td>
<td>If the port is assigned to the authorization VLAN as a tagged member, the PVID of the port does not change. The device maps the MAC address of each user to its own authorization VLAN.</td>
</tr>
</tbody>
</table>

**NOTE:**

An access port can be assigned to an authorization VLAN only as an untagged VLAN member.

| Hybrid port with MAC-based VLAN enabled | The device maps the MAC address of each user to its own authorization VLAN regardless of whether the port is a tagged member. The PVID of the port does not change. |

**IMPORTANT:**

- MAC authentication support for tagged VLAN assignment is available in Release 1121 and later.

- As a best practice, always assign a hybrid port to a VLAN as an untagged member. After the assignment, do not reconfigure the port as a tagged member in the VLAN.

Guest VLAN

You can configure a MAC authentication guest VLAN on a port to accommodate users that have failed MAC authentication on the port. Users in the MAC authentication guest VLAN can access a limited set of network resources, such as a software server, to download software and system patches. If no MAC authentication guest VLAN is configured, the users that have failed MAC authentication cannot access any network resources.
A hybrid port is always assigned to a MAC authentication guest VLAN as an untagged member. After the assignment, do not reconfigure the port as a tagged member in the VLAN.

Table 10 shows the way that the network access device handles guest VLANs for MAC authentication users.

### Table 10 VLAN manipulation

<table>
<thead>
<tr>
<th>Authentication status</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user in the MAC authentication guest VLAN fails MAC authentication for any other reason than server unreachable.</td>
<td>The user is still in the MAC authentication guest VLAN.</td>
</tr>
<tr>
<td>A user in the MAC authentication guest VLAN passes MAC authentication.</td>
<td>The device remaps the MAC address of the user to the authorization VLAN assigned by the authentication server. If no authorization VLAN is configured for the user on the authentication server, the device remaps the MAC address of the user to the PVID of the port.</td>
</tr>
</tbody>
</table>

### Critical VLAN

You can configure a MAC authentication critical VLAN on a port to accommodate users that fail MAC authentication because no RADIUS authentication server is reachable. Users in a MAC authentication critical VLAN can access only network resources in the critical VLAN.

The critical VLAN feature takes effect when MAC authentication is performed only through RADIUS servers. If a MAC authentication user fails local authentication after RADIUS authentication, the user is not assigned to the critical VLAN. For more information about the authentication methods, see "Configuring AAA."

Table 11 shows the way that the network access device handles critical VLANs for MAC authentication users.

### Table 11 VLAN manipulation

<table>
<thead>
<tr>
<th>Authentication status</th>
<th>VLAN manipulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>A user that has not been assigned to any VLAN fails MAC authentication because all the RADIUS servers are unreachable.</td>
<td>The device maps the MAC address of the user to the MAC authentication critical VLAN. The user is still in the MAC authentication critical VLAN if the user fails MAC reauthentication because all the RADIUS servers are unreachable.</td>
</tr>
<tr>
<td>A user in the MAC authentication critical VLAN fails MAC authentication for any other reason than server unreachable.</td>
<td>If a guest VLAN has been configured, the device maps the MAC address of the user to the guest VLAN. If no guest VLAN is configured, the device remaps the MAC address of the user to the PVID of the port.</td>
</tr>
<tr>
<td>A user in the MAC authentication critical VLAN passes MAC authentication.</td>
<td>The device remaps the MAC address of the user to the authorization VLAN assigned by the authentication server. If no authorization VLAN is configured for the user on the authentication server, the device remaps the MAC address of the user to the PVID of the access port.</td>
</tr>
</tbody>
</table>

### ACL assignment

You can specify an authorization ACL in the user account for a MAC authentication user to control the user’s access to network resources. After the user passes MAC authentication, the authentication server (local or remote) assigns the authorization ACL to the access port of the user.
The ACL will filter traffic for this user. You must configure ACL rules for the authorization ACL on the access device for the ACL assignment feature.

To ensure a successful ACL assignment, make sure the ACL does not contain rules that match source MAC addresses.

To change the access control criteria for the user, you can use one of the following methods:

- Modify ACL rules on the access device.
- Specify another authorization ACL on the authentication server.

For more information about ACLs, see *ACL and QoS Configuration Guide*.

## User profile assignment

You can specify a user profile in the user account for a MAC authentication user to control the user's access to network resources. After the user passes MAC authentication, the authentication server assigns the user profile to the user to filter traffic for this user. The authentication server can be the local access device or a RADIUS server. In either case, you must configure the user profile on the access device.

To change the user's access permissions, you can use one of the following methods:

- Modify the user profile configuration on the access device.
- Specify another user profile for the user on the authentication server.

For more information about user profiles, see "Configuring user profiles."

## Periodic MAC reauthentication

**IMPORTANT:**

This feature is available in Release 1121 and later.

Periodic MAC reauthentication tracks the connection status of online users, and updates the authorization attributes assigned by the RADIUS server. The attributes include the ACL and VLAN.

The device reauthenticate an online MAC authentication user periodically only after it receives termination action Radius-request from the authentication server for this user. The Session-Timeout attribute (session timeout period) assigned by the server is the reauthentication interval. To display the server-assigned Session-Timeout and Termination-Action attributes, use the `display mac-authentication connection` command. Support for the server configuration and assignment of Session-Timeout and Termination-Action attributes depends on the server model.

When no server is reachable for MAC reauthentication, the device keeps the MAC authentication users online or logs off the users, depending on the keep-online feature configuration on the device. For information about the keep-online feature, see "Configuring the keep-online feature."

## Configuration prerequisites

Before you configure MAC authentication, complete the following tasks:

1. Configure an ISP domain and specify an AAA method. For more information, see "Configuring AAA."
   - For local authentication, you must also create local user accounts (including usernames and passwords), and specify the lan-access service for local users.
   - For RADIUS authentication, make sure the device and the RADIUS server can reach each other, and create user accounts on the RADIUS server. If you are using MAC-based accounts, make sure the username and password for each account are the same as the MAC address of each MAC authentication user.
2. Make sure the port security feature is disabled. For more information about port security, see "Configuring port security."

Configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling MAC authentication</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Specifying a MAC authentication domain</td>
<td>mac-authentication</td>
<td>By default, MAC authentication is disabled globally.</td>
</tr>
<tr>
<td>(Optional.) Configuring the user account format</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Configuring MAC authentication timers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Setting the maximum number of concurrent MAC authentication users on a port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Enabling MAC authentication multi-VLAN mode on a port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring MAC authentication delay</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Enabling parallel processing of MAC authentication and 802.1X authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring a MAC authentication guest VLAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring a MAC authentication critical VLAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Enabling the MAC authentication critical voice VLAN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring the keep-online feature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional.) Enabling MAC authentication offline detection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enabling MAC authentication

For MAC authentication to take effect on a port, you must enable the feature globally and on the port. MAC authentication is exclusive with link aggregation group or service loopback group.

- You cannot enable MAC authentication on a port already in a link aggregation group or a service loopback group.
- You cannot add a MAC authentication-enabled port to a link aggregation group or a service loopback group.

To enable MAC authentication:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable MAC authentication globally.</td>
<td>mac-authentication</td>
<td>By default, MAC authentication is disabled globally.</td>
</tr>
<tr>
<td>3. Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>4. Enable MAC authentication on the port.</td>
<td>mac-authentication</td>
<td>By default, MAC authentication is disabled on a port.</td>
</tr>
</tbody>
</table>
Specifying a MAC authentication domain

By default, MAC authentication users are in the system default authentication domain. To implement different access policies for users, you can use one of the following methods to specify authentication domains for MAC authentication users:

- Specify a global authentication domain in system view. This domain setting applies to all ports enabled with MAC authentication.
- Specify an authentication domain for an individual port in Layer 2 Ethernet interface view.

MAC authentication chooses an authentication domain for users on a port in this order: the port-specific domain, the global domain, and the default domain. For more information about authentication domains, see "Configuring AAA."

To specify an authentication domain for MAC authentication users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Specify an authentication domain for MAC authentication users. | • In system view: mac-authentication domain domain-name  
• In Layer 2 Ethernet interface view:  
  a. interface interface-type interface-number  
  b. mac-authentication domain domain-name | By default, the system default authentication domain is used for MAC authentication users. |

Configuring the user account format

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Configure the MAC authentication user account format. | • Use one MAC-based user account for each user: mac-authentication user-name-format mac-address [ { with-hyphen | without-hyphen } [ lowercase | uppercase ] ]  
• Use one shared user account for all users:  
mac-authentication user-name-format fixed [ account name ] [ password { cipher | simple } password ] | By default, the device uses the MAC address of a user as the username and password for MAC authentication. The MAC address is in the hexadecimal notation without hyphens, and letters are in lower case. |

Configuring MAC authentication timers

MAC authentication uses the following timers:

- **Offline detect timer**—Sets the interval that the device waits for traffic from a user before the device regards the user idle. If a user connection has been idle within the interval, the device
logs the user out and stops accounting for the user. In Release 1121 and later, this timer takes effect when the MAC authentication offline detection feature is enabled.

After you set the offline detect timer, assign the same value to the MAC address aging timer by using the `mac-address timer` command. This operation prevents a MAC authenticated user from being offline within the offline detect timer due to MAC address entry expiration.

- **Quiet timer**—Sets the interval that the device must wait before the device can perform MAC authentication for a user who has failed MAC authentication. All packets from the MAC address are dropped during the quiet time. This quiet mechanism prevents repeated authentication from affecting system performance.
- **Server timeout timer**—Sets the interval that the device waits for a response from a RADIUS server before the device regards the RADIUS server unavailable. If the timer expires during MAC authentication, the user cannot access the network.

To configure MAC authentication timers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure MAC authentication timers.</td>
<td>`mac-authentication timer { offline-detect offline-detect-value</td>
</tr>
</tbody>
</table>

**Setting the maximum number of concurrent MAC authentication users on a port**

Perform this task to prevent the system resources from being overused.

To set the maximum number of concurrent MAC authentication users on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>3.</td>
<td>Set the maximum number of concurrent MAC authentication users on the port</td>
<td><code>mac-authentication max-user user-number</code></td>
</tr>
</tbody>
</table>

**Enabling MAC authentication multi-VLAN mode on a port**

The MAC authentication multi-VLAN mode prevents an authenticated online user from service interruption caused by VLAN changes on a port. When the port receives a packet sourced from the user in a VLAN not matching the existing MAC-VLAN mapping, the device neither logs off the user nor reauthenticates the user. The device creates a new MAC-VLAN mapping for the user, and traffic transmission is not interrupted. The original MAC-VLAN mapping for the user remains on the device until it dynamically ages out. As a best practice, configure this feature on hybrid or trunk ports.
This feature improves transmission of data that is vulnerable to delay and interference. It is typically applicable to IP phone users.

To enable MAC authentication multi-VLAN mode on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable MAC authentication multi-VLAN mode.</td>
<td>mac-authentication host-mode multi-vlan</td>
</tr>
</tbody>
</table>

### Configuring MAC authentication delay

When both 802.1X authentication and MAC authentication are enabled on a port, you can delay MAC authentication so that 802.1X authentication is preferentially triggered.

If no 802.1X authentication is triggered or 802.1X authentication fails within the delay period, the port continues to process MAC authentication.

Do not set the port security mode to `mac-else-userlogin-secure` or `mac-else-userlogin-secure-ext` when you use MAC authentication delay. The delay does not take effect on a port in either of the two modes. For more information about port security modes, see "Configuring port security."

To configure MAC authentication delay:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable MAC authentication delay and set the delay timer.</td>
<td>mac-authentication auth-delay time</td>
</tr>
</tbody>
</table>

### Enabling parallel processing of MAC authentication and 802.1X authentication

**IMPORTANT:**
This feature is available in Release 1121 and later.

This feature enables a port that processes MAC authentication after 802.1X authentication is finished to process MAC authentication in parallel with 802.1X authentication.

When the port receives a packet from an unknown MAC address, it sends a unicast EAP-Request/Identity packet to the MAC address. After that, the port immediately processes MAC authentication without waiting for the 802.1X authentication result.
After MAC authentication succeeds, the port is assigned to the MAC authentication authorization VLAN.

- If 802.1X authentication fails, the MAC authentication result takes effect.
- If 802.1X authentication succeeds, the device handles the port and the MAC address based on the 802.1X authentication result.

Configuration restrictions and guidelines

When you enable parallel processing of MAC authentication and 802.1X authentication on a port, follow these restrictions and guidelines:

- Make sure the port meets the following requirements:
  - The port is configured with both 802.1X authentication and MAC authentication and performs MAC-based access control for 802.1X authentication.
  - The port is enabled with the 802.1X unicast trigger.
- For the port to perform MAC authentication before it is assigned to the 802.1X guest VLAN, enable 802.1X guest VLAN assignment delay.
  For information about 802.1X guest VLAN assignment delay, see "Configuring 802.1X."
- For the parallel processing feature to work correctly, do not enable MAC authentication delay on the port. This operation will delay MAC authentication after 802.1X authentication is triggered.
- To configure both 802.1X authentication and MAC authentication on the port, use one of the following methods:
  - Enable the 802.1X and MAC authentication features separately on the port.
  - Enable port security on the port. The port security mode must be `userlogin-secure-or-mac` or `userlogin-secure-or-mac-ext`.
    For information about port security mode configuration, see "Configuring port security."

Configuration procedure

To enable parallel processing of MAC authentication and 802.1X authentication on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>mac-authentication parallel-with-dot1x</td>
<td>By default, this feature is disabled.</td>
</tr>
</tbody>
</table>

Configuring a MAC authentication guest VLAN

You must configure the MAC authentication guest VLAN on a hybrid port. Before you configure the MAC authentication guest VLAN on a hybrid port, complete the following tasks:

- Enable MAC authentication globally and on the port.
- Enable MAC-based VLAN on the port.
- Create the VLAN to be specified as the MAC authentication guest VLAN.
- Configure the VLAN as an untagged member on the port.
When you configure the MAC authentication guest VLAN on a port, follow the guidelines in Table 12.

### Table 12 Relationships of the MAC authentication guest VLAN with other security features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Relationship description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet feature of MAC authentication</td>
<td>The MAC authentication guest VLAN feature has higher priority. When a user fails MAC authentication, the user can access the resources in the guest VLAN. The user's MAC address is not marked as a silent MAC address.</td>
<td>See &quot;Configuring MAC authentication timers.&quot;</td>
</tr>
<tr>
<td>Super VLAN</td>
<td>You cannot specify a VLAN as both a super VLAN and a MAC authentication guest VLAN.</td>
<td>See Layer 2—LAN Switching Configuration Guide.</td>
</tr>
<tr>
<td>Port intrusion protection</td>
<td>The guest VLAN feature has higher priority than the block MAC action but lower priority than the shutdown port action of the port intrusion protection feature.</td>
<td>See &quot;Configuring port security.&quot;</td>
</tr>
</tbody>
</table>

To configure the MAC authentication guest VLAN on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view. interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the MAC authentication guest VLAN on the port. mac-authentication guest-vlan guest-vlan-id</td>
<td>By default, no MAC authentication guest VLAN is specified on a port. You can configure only one MAC authentication guest VLAN on a port.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Set the authentication interval for users in the MAC authentication guest VLAN. mac-authentication guest-vlan auth-period period-value</td>
<td>The default setting is 30 seconds. This command is available in Release 1121 and later.</td>
</tr>
</tbody>
</table>

### Configuring a MAC authentication critical VLAN

You must configure the MAC authentication critical VLAN on a hybrid port. Before you configure the MAC authentication critical VLAN on a hybrid port, complete the following tasks:

- Enable MAC authentication globally and on the port.
- Enable MAC-based VLAN on the port.
- Create the VLAN to be specified as the MAC authentication critical VLAN.
- Configure the VLAN as an untagged member on the port.

When you configure the MAC authentication critical VLAN on a port, follow the guidelines in Table 13.
Table 13 Relationships of the MAC authentication critical VLAN with other security features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Relationship description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quiet feature of MAC authentication</td>
<td>The MAC authentication critical VLAN feature has higher priority. When a user fails MAC authentication because no RADIUS authentication server is reachable, the user can access the resources in the critical VLAN. The user's MAC address is not marked as a silent MAC address.</td>
<td>See &quot;Configuring MAC authentication timers.&quot;</td>
</tr>
<tr>
<td>Super VLAN</td>
<td>You cannot specify a VLAN as both a super VLAN and a MAC authentication critical VLAN.</td>
<td>See Layer 2—LAN Switching Configuration Guide.</td>
</tr>
<tr>
<td>Port intrusion protection</td>
<td>The critical VLAN feature has higher priority than the block MAC action but lower priority than the shutdown port action of the port intrusion protection feature.</td>
<td>See &quot;Configuring port security.&quot;</td>
</tr>
</tbody>
</table>

To configure the MAC authentication critical VLAN on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the MAC authentication critical VLAN on the port.</td>
<td>mac-authentication critical vlan critical-vlan-id By default, no MAC authentication critical VLAN is specified on a port. You can configure only one MAC authentication critical VLAN on a port.</td>
</tr>
</tbody>
</table>

Enabling the MAC authentication critical voice VLAN

**IMPORTANT:**
This feature is available in Release 1121 and later.

The MAC authentication critical voice VLAN on a port accommodates MAC authentication voice users who have failed authentication because none of the RADIUS servers in their ISP domain are reachable.

Configuration prerequisites

Before you enable the MAC authentication critical voice VLAN on a port, complete the following tasks:

- Enable LLDP both globally and on the port.
  - The device uses LLDP to identify voice users. For information about LLDP, see Layer 2—LAN Switching Configuration Guide.
- Enable voice VLAN on the port.
For information about voice VLANs, see *Layer 2—LAN Switching Configuration Guide*.

**Configuration procedure**

To enable the MAC authentication critical voice VLAN feature on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the MAC authentication critical voice VLAN feature on a port.</td>
<td>mac-authentication critical-voice-vlan</td>
</tr>
</tbody>
</table>

**Configuring the keep-online feature**

By default, the device logs off online MAC authentication users if no server is reachable for MAC reauthentication. The keep-online feature keeps authenticated MAC authentication users online when no server is reachable for MAC reauthentication.

In a fast-recovery network, you can use the keep-online feature to prevent MAC authentication users from coming online and going offline frequently.

To configure the keep-online feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the keep-online feature for authenticated MAC authentication users on the port.</td>
<td>mac-authentication re-authenticate server-unreachable keep-online</td>
</tr>
</tbody>
</table>

**Enabling MAC authentication offline detection**

**IMPORTANT:**
This feature is available in Release 1121 and later.

This feature logs a user out of the device if the device does not receive any packets from the user within the offline detect timer. The device also requests to stop accounting for the user at the same time. For more information about the offline detect timer, see "Configuring MAC authentication timers."

Disabling this feature disables the device from inspecting the online user status.

To enable MAC authentication offline detection:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Enable MAC authentication offline detection.</td>
<td>mac-authentication offline-detect enable</td>
<td>By default, MAC authentication offline detection is enabled.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining MAC authentication

**IMPORTANT:**
The `reset mac-authentication critical-voice-vlan interface interface-type interface-number [mac-address mac-address]` command is available in Release 1121 and later.

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display MAC authentication information.</td>
<td><code>display mac-authentication [interface interface-type interface-number]</code></td>
</tr>
<tr>
<td>Display MAC authentication connections.</td>
<td>`display mac-authentication connection [interface interface-type interface-number</td>
</tr>
<tr>
<td>Clear MAC authentication statistics.</td>
<td><code>reset mac-authentication statistics [interface interface-type interface-number]</code></td>
</tr>
<tr>
<td>Remove users from the MAC authentication critical VLAN on a port.</td>
<td><code>reset mac-authentication critical-vlan interface interface-type interface-number [mac-address mac-address]</code></td>
</tr>
<tr>
<td>Remove users from the MAC authentication critical voice VLAN on a port.</td>
<td><code>reset mac-authentication critical-voice-vlan interface interface-type interface-number [mac-address mac-address]</code></td>
</tr>
<tr>
<td>Remove users from the MAC authentication guest VLAN on a port.</td>
<td><code>reset mac-authentication guest-vlan interface interface-type interface-number [mac-address mac-address]</code></td>
</tr>
</tbody>
</table>

### MAC authentication configuration examples

#### Local MAC authentication configuration example

**Network requirements**

As shown in Figure 35, the device performs local MAC authentication on GigabitEthernet 1/0/1 to control Internet access of users.

Configure the device to meet the following requirements:
- Detect whether a user has gone offline every 180 seconds.
- Deny a user for 180 seconds if the user fails MAC authentication.
- Authenticate all users in ISP domain **bbb**.
Use the MAC address of each user as the username and password for authentication. A MAC address is in the hexadecimal notation with hyphens, and letters are in lower case.

**Figure 35 Network diagram**

```
Host A
MAC: 00-e0-fc-12-34-56

GE1/0/1

Device

IP network

Host B
MAC: 00-e0-fc-11-11-11
```

**Configuration procedure**

`# Add a network access local user. In this example, configure both the username and password as Host A’s MAC address 00-e0-fc-12-34-56.`

```
<Device> system-view

[Device] local-user 00-e0-fc-12-34-56 class network
[Device-luser-network-00-e0-fc-12-34-56] password simple 00-e0-fc-12-34-56

# Specify the LAN access service for the user.
[Device-luser-network-00-e0-fc-12-34-56] service-type lan-access
[Device-luser-network-00-e0-fc-12-34-56] quit

# Configure ISP domain bbb to perform local authentication for LAN users.
[Device] domain bbb
[Device-isp-bbb] authentication lan-access local
[Device-isp-bbb] quit

# Enable MAC authentication on port GigabitEthernet 1/0/1.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit

# Specify the MAC authentication domain as the ISP domain bbb.
[Device] mac-authentication domain bbb

# Configure MAC authentication timers.
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180

# Configure MAC authentication to use MAC-based accounts. Each MAC address is in the hexadecimal notation with hyphens, and letters are in lower case.
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase

# Enable MAC authentication globally.
[Device] mac-authentication
```

**Verifying the configuration**

`# Display MAC authentication settings and statistics to verify your configuration.`

```
[Device] display mac-authentication

Global MAC authentication parameters:
MAC authentication : Enabled
User name format    : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
Username            : mac
Password            : Not configured
```
Offline detect period : 180 s
Quiet period : 180 s
Server timeout : 100 s
Authentication domain : bbb
Max MAC-auth users : 2048 per slot
Online MAC-auth users : 1

Silent MAC users:
<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN ID</th>
<th>From port</th>
<th>Port index</th>
</tr>
</thead>
<tbody>
<tr>
<td>00e0-fc11-1111</td>
<td>8</td>
<td>GigabitEthernet1/0/1</td>
<td>1</td>
</tr>
</tbody>
</table>

GigabitEthernet1/0/1 is link-up
MAC authentication : Enabled
Authentication domain : Not configured
Auth-delay timer : Disabled
Re-auth server-unreachable : Logoff
Guest VLAN : Not configured
Guest VLAN auth-period : 30 s
Critical VLAN : Not configured
Critical voice VLAN : Disabled
Host mode : Single VLAN
Offline detection : Enabled
Authentication order : Default

Max online users : 2048
Authentication attempts : successful 1, failed 0
Current online users : 1
<table>
<thead>
<tr>
<th>MAC address</th>
<th>Auth state</th>
</tr>
</thead>
<tbody>
<tr>
<td>00e0-fc12-3456</td>
<td>Authenticated</td>
</tr>
</tbody>
</table>

The output shows that Host A has passed MAC authentication and has come online. Host B failed MAC authentication and its MAC address is marked as a silent MAC address.

RADIUS-based MAC authentication configuration example

Network requirements
As shown in Figure 36, the device uses RADIUS servers to perform authentication, authorization, and accounting for users.

To control user access to the Internet by MAC authentication, perform the following tasks:
- Enable MAC authentication globally and on port GigabitEthernet 1/0/1.
- Configure the device to detect whether a user has gone offline every 180 seconds.
- Configure the device to deny a user for 180 seconds if the user fails MAC authentication.
- Configure all users to belong to the ISP domain bbb.
- Use a shared user account for all users, with the username aaa and password 123456.
Figure 36 Network diagram

Configuration procedure

1. Make sure the RADIUS server and the access device can reach each other. (Details not shown.)
2. Configure the RADIUS servers:
   # Create a shared account for MAC authentication users. (Details not shown.)
   # Set the username aaa and password 123456 for the account. (Details not shown.)
3. Configure RADIUS-based MAC authentication on the device:
   # Configure a RADIUS scheme.
   `<Device> system-view
   [Device] radius scheme 2000
   [Device-radius-2000] primary authentication 10.1.1.1 1812
   [Device-radius-2000] primary accounting 10.1.1.2 1813
   [Device-radius-2000] key authentication simple abc
   [Device-radius-2000] key accounting simple abc
   [Device-radius-2000] user-name-format without-domain
   [Device-radius-2000] quit
   # Apply the RADIUS scheme to ISP domain bbb for authentication, authorization, and accounting.
   [Device] domain bbb
   [Device-isp-bbb] authentication default radius-scheme 2000
   [Device-isp-bbb] authorization default radius-scheme 2000
   [Device-isp-bbb] quit
   # Enable MAC authentication on port GigabitEthernet 1/0/1.
   [Device] interface gigabitethernet 1/0/1
   [Device-GigabitEthernet1/0/1] mac-authentication
   [Device-GigabitEthernet1/0/1] quit
   # Specify the MAC authentication domain as the ISP domain bbb.
   [Device] mac-authentication domain bbb
   # Set MAC authentication timers.
   [Device] mac-authentication timer offline-detect 180
   [Device] mac-authentication timer quiet 180
   # Specify username aaa and password 123456 in plain text for the account shared by MAC authentication users.
   [Device] mac-authentication user-name-format fixed account aaa password simple 123456
   # Enable MAC authentication globally.
Verifying the configuration

# Verify the MAC authentication configuration.

[Device] display mac-authentication

Global MAC authentication parameters:
- MAC authentication : Enabled
- Username format : Fixed account
  - Username : aaa
  - Password : *****
- Offline detect period : 180 s
- Quiet period : 180 s
- Server timeout : 100 s
- Authentication domain : bbb
- Max MAC-auth users : 2048 per slot
- Online MAC-auth users : 1

Silent MAC users:

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN ID</th>
<th>From port</th>
<th>Port index</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GigabitEthernet1/0/1 is link-up
- MAC authentication : Enabled
- Authentication domain : Not configured
- Auth-delay timer : Disabled
- Re-auth server-unreachable : Logoff
- Guest VLAN : Not configured
- Guest VLAN auth-period : 30 s
- Critical VLAN : Not configured
- Critical voice VLAN : Disabled
- Host mode : Single VLAN
- Offline detection : Enabled
- Authentication order : Default
- Max online users : 2048
- Authentication attempts : successful 1, failed 0
- Current online users : 1
  - MAC address : 00e0-fc12-3456
  - Auth state : Authenticated

ACL assignment configuration example

Network requirements

As shown in Figure 37, configure the device to meet the following requirements:
- Use RADIUS servers to perform authentication, authorization, and accounting for users.
- Perform MAC authentication on port GigabitEthernet 1/0/1 to control Internet access.
- Use MAC-based user accounts for MAC authentication users. Each MAC address is in the hexadecimal notation with hyphens, and letters are in lower case.
- Use an ACL to deny authenticated users to access the FTP server at 10.0.0.1.
Configuration procedure

Make sure the RADIUS servers and the access device can reach each other.

1. Configure ACL 3000 to deny packets destined for 10.0.0.1.

   <Sysname> system-view
   [Sysname] acl number 3000
   [Sysname-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
   [Sysname-acl-adv-3000] quit

2. Configure RADIUS-based MAC authentication on the device:

   # Configure a RADIUS scheme.
   [Sysname] radius scheme 2000
   [Sysname-radius-2000] primary authentication 10.1.1.1 1812
   [Sysname-radius-2000] primary accounting 10.1.1.2 1813
   [Sysname-radius-2000] key authentication simple abc
   [Sysname-radius-2000] key accounting simple abc
   [Sysname-radius-2000] user-name-format without-domain
   [Sysname-radius-2000] quit

   # Apply RADIUS scheme 2000 to ISP domain 2000 for authentication, authorization, and accounting.
   [Sysname] domain 2000
   [Sysname-isp-2000] quit

   # Specify the ISP domain for MAC authentication.
   [Sysname] mac-authentication domain 2000

   # Configure the device to use MAC-based user accounts. Each MAC address is in the hexadecimal notation with hyphens, and letters are in lower case.
   [Sysname] mac-authentication user-name-format mac-address with-hyphen lowercase

   # Enable MAC authentication on port GigabitEthernet 1/0/1.
   [Sysname] interface gigabitethernet 1/0/1
   [Sysname-GigabitEthernet1/0/1] mac-authentication
   [Sysname-GigabitEthernet1/0/1] quit

   # Enable MAC authentication globally.
   [Sysname] mac-authentication
3. Configure the RADIUS servers:
   
   # Add a user account with 00-e0-fc-12-34-56 as both the username and password on each
   RADIUS server. (Details not shown.)
   
   # Authorize ACL 3000 to the user account. (Details not shown.)

Verifying the configuration

# Verify the MAC authentication configuration.

[Sysname] display mac-authentication

Global MAC authentication parameters:

  MAC authentication : Enabled
  Username format    : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
  Username           : mac
  Password           : Not configured
  Offline detect period : 180 s
  Quiet period       : 180 s
  Server timeout     : 100 s
  Authentication domain : 2000
  Max MAC-auth users : 2048 per slot
  Online MAC-auth users : 1

Silent MAC users:

  MAC address  VLAN ID  From port  Port index

  00e0-fc12-3456    Authenticated

GigabitEthernet1/0/1 is link-up

  MAC authentication : Enabled
  Authentication domain : Not configured
  Auth-delay timer    : Disabled
  Re-auth server-unreachable : Logoff
  Guest VLAN         : Not configured
  Guest VLAN auth-period : 30 s
  Critical VLAN      : Not configured
  Critical voice VLAN : Disabled
  Host mode          : Single VLAN
  Offline detection  : Enabled
  Authentication order : Default

  Max online users : 2048
  Authentication attempts : successful 1, failed 0
  Current online users : 1

# Verify that you cannot ping the FTP server from the host.

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

  Request timed out.
  Request timed out.
  Request timed out.
Request timed out.

Ping statistics for 10.0.0.1:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

The output shows that ACL 3000 has been assigned to port GigabitEthernet 1/0/1 to deny access to the FTP server.
Configuring portal authentication

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces.

Overview

Portal authentication controls user access to the Internet. Portal authenticates a user by the username and password the user enters on a portal authentication page. Therefore, portal authentication is also known as Web authentication. When portal authentication is deployed on a network, an access device redirects unauthenticated users to the website provided by a portal Web server. The users can access the resources on the website without authentication. If the users want to access the Internet, they must pass authentication on the website.

Portal authentication is classified into the following types:

- **Active authentication**—Users visit the authentication website provided by the portal Web server and enter their username and password for authentication.
- **Forced authentication**—Users are redirected to the portal authentication website for authentication when they visit other websites.

Portal authentication flexibly imposes access control on the access layer and vital data entries. It has the following advantages:

- Allows users to perform authentication through Web pages without installing client software.
- Provides ISPs with diversified management choices and extended functions. For example, the ISPs can place advertisements, provide community services, and publish information on the authentication page.
- Supports multiple authentication modes. For example, re-DHCP authentication implements a flexible address assignment scheme and saves public IP addresses. Cross-subnet authentication can authenticate users who reside in a different subnet than the access device.

The device supports Portal 1.0, Portal 2.0, and Portal 3.0.

Extended portal functions

By forcing patching and anti-virus policies, extended portal functions help hosts to defend against viruses. Portal supports the following extended functions:

- **Security check**—Detects after authentication whether or not a user host installs anti-virus software, virus definition file, unauthorized software, and operating system patches.
- **Resource access restriction**—Allows an authenticated user to access certain network resources such as the virus server and the patch server. Users can access more Internet resources after passing security check.

Security check must cooperate with the HPE IMC security policy server and the iNode client.

Portal system components

A typical portal system consists of these basic components: authentication client, access device, portal authentication server, portal Web server, AAA server, and security policy server.
Authentication client
An authentication client is a Web browser that runs HTTP/HTTPS or a user host that runs a portal client application. Security check for the user host is implemented through the interaction between the portal client and the security policy server.

Access device
An access device refers to a broadband access device such as a switch or a router. An access device has the following functions:
- Redirects all HTTP requests of unauthenticated users to the portal Web server.
- Interacts with the portal authentication server and the AAA server to complete authentication, authorization, and accounting.
- Allows users that pass portal authentication to access authorized Internet resources.

Portal authentication server
The portal authentication server receives authentication requests from authentication clients and interacts with the access device to authenticate users.

Portal Web server
The portal Web server pushes the Web authentication page to authentication clients and forwards user authentication information (username and password) to the portal authentication server. The access device also redirects HTTP requests from unauthenticated users to the portal Web server.

The portal Web server can be integrated with the portal authentication server or an independent server.

AAA server
The AAA server interacts with the access device to implement authentication, authorization, accounting for portal users. Now only a RADIUS server can act as an AAA server in a portal system.

Security policy server
The security policy server interacts with the portal client and the access device for security check and authorization for users.
Portal system using the local portal Web server

**IMPORTANT:**
This feature is available in Release 1121 and later.

The access device supports the local portal Web server feature. Using this feature, the access device also acts as the portal Web server and the portal authentication server to perform local portal authentication on portal users. In this case, the portal system consists of only three components: authentication client, access device, and authentication/accounting server, as shown in Figure 39.

**Figure 39 Portal system using the local portal Web server**

The authentication client cannot be an HPE iNode client. Local portal authentication only supports authenticating Web clients.

No security policy server is needed because local portal authentication does not support extended portal functions.

The local portal Web server feature implements only some simple portal server functions. It only allows users to log in and log out through the Web interface. It cannot take the place of independent portal Web and authentication servers.

**Client and local portal Web server interaction protocols**

HTTP and HTTPS can be used for interaction between an authentication client and a local portal Web server. If HTTP is used, there are potential security problems because HTTP packets are transferred in plain text. If HTTPS is used, secure data transmission is ensured because HTTP packets are secured by SSL.

**Portal page customization**

To perform local portal authentication, you must customize a set of authentication pages that the device will push to users. You can customize multiple sets of authentication pages, compress each set of the pages to a .zip file, and upload the compressed files to the storage medium of the device. On the device, you must specify one of the files as the default authentication page file by using the `default-logon-page` command.

For more information about authentication page customization, see "Customizing authentication pages." For more information about the `default-logon-page` command, see Security Command Reference.

**Interaction between portal system components**

The components of a portal system interact as follows:

1. An unauthenticated user initiates authentication by accessing an Internet website through a Web browser. When receiving the HTTP request, the access device redirects it to the Web authentication page provided by the portal Web server. The user can also visit the authentication website to log in. The user must log in through the HPE iNode client for extended portal functions.

2. The user enters the authentication information on the authentication page/dialog box and submits the information. The portal Web server forwards the information to the portal
authentication server. Then the portal authentication server processes the information and forwards it to the access device.

3. The access device interacts with the AAA server to implement authentication, authorization, accounting for the user.

4. If security policies are not imposed on the user, the access device allows the authenticated user to access the Internet. If security policies are imposed on the user, the portal client, the access device, and the security policy server interact to check the user host. If the user passes the security check, the security policy server authorizes the user to access resources based on the check result. Portal authentication through Web does not support security check for users. To implement security check, the client must be the HPE iNode client.

NOTE:
Portal authentication supports NAT traversal whether it is initiated by a Web client or an HPE iNode client. NAT traversal must be configured when the portal client is on a private network and the portal server is on a public network.

Portal authentication modes

Portal authentication has three modes: direct authentication, re-DHCP authentication, and cross-subnet authentication. In direct authentication and re-DHCP authentication, no Layer 3 forwarding devices exist between the authentication client and the access device. In cross-subnet authentication, Layer 3 forwarding devices can exist between the authentication client and the access device.

Direct authentication

A user manually configures a public IP address or obtains a public IP address through DHCP. Before authentication, the user can access only the portal Web server and predefined authentication-free websites. After passing authentication, the user can access other network resources. The process of direct authentication is simpler than that of re-DHCP authentication.

Re-DHCP authentication

Before a user passes authentication, DHCP allocates an IP address (a private IP address) to the user. The user can access only the portal Web server and predefined authentication-free websites. After the user passes authentication, DHCP reallocates an IP address (a public IP address) to the user. The user then can access other network resources. No public IP address is allocated to users who fail authentication. Re-DHCP authentication saves public IP addresses. For example, an ISP can allocate public IP addresses to broadband users only when they access networks beyond the residential community network.

Only the HPE iNode client supports re-DHCP authentication. IPv6 portal authentication does not support the re-DHCP authentication mode.

Cross-subnet authentication

Cross-subnet authentication is similar to direct authentication, except it allows Layer 3 forwarding devices to exist between the authentication client and the access device.

In direct authentication, re-DHCP authentication, and cross-subnet authentication, a user’s IP address uniquely identifies the user. After a user passes authentication, the access device generates an ACL for the user based on the user’s IP address to control forwarding of the packets from the user. Because no Layer 3 forwarding device exists between authentication clients and the access device in direct authentication and re-DHCP authentication, the access device can learn the user MAC addresses. The access device can enhance its capability of controlling packet forwarding by using the learned MAC addresses.
Portal authentication process

Direct authentication and cross-subnet authentication share the same authentication process. Re-DHCP authentication has a different process as it has two address allocation procedures.

Direct authentication/cross-subnet authentication process (with CHAP/PAP authentication)

Figure 40 Direct authentication/cross-subnet authentication process

The direct/cross-subnet authentication process is as follows:

1. A portal user access the Internet through HTTP, and the HTTP packet arrives at the access device.
   - If the packet matches a portal free rule, the access device allows the packet to pass.
   - If the packet does not match any portal-free rule, the access device redirects the packet to the portal Web server. The portal Web server pushes the Web authentication page to the user for him to enter his username and password.

2. The portal Web server submits the user authentication information to the portal authentication server.

3. The portal authentication server and the access device exchange CHAP messages. This step is skipped for PAP authentication. The portal authentication server decides the method (CHAP or PAP) to use.

4. The portal authentication server adds the username and password into an authentication request packet and sends it to the access device. Meanwhile, the portal authentication server starts a timer to wait for an authentication reply packet.

5. The access device and the RADIUS server exchange RADIUS packets.

6. The access device sends an authentication reply packet to the portal authentication server to notify authentication success or failure.

7. The portal authentication server sends an authentication success or failure packet to the client.

8. If the authentication is successful, the portal authentication server sends an authentication reply acknowledgment packet to the access device.

If the client is an iNode client, the authentication process includes step 9 and step 10 for extended portal functions. Otherwise the authentication process is complete.

9. The client and the security policy server exchange security check information. The security policy server detects whether or not the user host installs anti-virus software, virus definition files, unauthorized software, and operating system patches.
10. The security policy server authorizes the user to access certain network resources based on the check result. The access device saves the authorization information and uses it to control access of the user.

Re-DHCP authentication process (with CHAP/PAP authentication)

Figure 41 Re-DHCP authentication process

The re-DHCP authentication process is as follows:

Step 1 through step 7 are the same as those in the direct authentication/cross-subnet authentication process.

8. After receiving the authentication success packet, the client obtains a public IP address through DHCP. The client then notifies the portal authentication server that it has a public IP address.

9. The portal authentication server notifies the access device that the client has obtained a public IP address.

10. The access device detects the IP change of the client through DHCP and then notifies the portal authentication server that it has detected an IP change of the client IP.

11. After receiving the IP change notification packets sent by the client and the access device, the portal authentication server notifies the client of login success.

12. The portal authentication server sends an IP change acknowledgment packet to the access device.

Step 13 and step 14 are for extended portal functions.

13. The client and the security policy server exchanges security check information. The security policy server detects whether or not the user host installs anti-virus software, virus definition files, unauthorized software, and operating system patches.

14. The security policy server authorizes the user to access certain network resources based on the check result. The access device saves the authorization information and uses it to control access of the user.
# Portal configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring a portal authentication server</td>
</tr>
<tr>
<td>(Required.) Configuring a portal Web server</td>
</tr>
<tr>
<td>(Required.) Enabling portal authentication on an interface</td>
</tr>
<tr>
<td>(Required.) Referencing a portal Web server for an interface</td>
</tr>
<tr>
<td>(Optional.) Controlling portal user access</td>
</tr>
<tr>
<td>• Configuring a portal-free rule</td>
</tr>
<tr>
<td>• Configuring an authentication source subnet</td>
</tr>
<tr>
<td>• Configuring an authentication destination subnet</td>
</tr>
<tr>
<td>• Setting the maximum number of portal users</td>
</tr>
<tr>
<td>• Specifying a portal authentication domain</td>
</tr>
<tr>
<td>(Optional.) Configuring portal detection features</td>
</tr>
<tr>
<td>• Configuring online detection of portal users</td>
</tr>
<tr>
<td>• Configuring portal authentication server detection</td>
</tr>
<tr>
<td>• Configuring portal Web server detection</td>
</tr>
<tr>
<td>• Configuring portal user synchronization</td>
</tr>
<tr>
<td>(Optional.) Configuring the portal fail-permit feature</td>
</tr>
<tr>
<td>(Optional.) Configuring BAS-IP for portal packets sent to the portal authentication server</td>
</tr>
<tr>
<td>(Optional.) Applying a NAS-ID profile to an interface</td>
</tr>
<tr>
<td>(Optional.) Enabling portal roaming</td>
</tr>
<tr>
<td>(Optional.) Logging out portal users</td>
</tr>
<tr>
<td>(Optional) Configuring the local portal Web server feature</td>
</tr>
</tbody>
</table>

## Configuration prerequisites

The portal feature provides a solution for user identity authentication and security check. To complete user identity authentication, portal must cooperate with RADIUS.

The prerequisites for portal authentication configuration are as follows:

- The portal authentication server, portal Web server, and RADIUS server have been installed and configured properly.
- To use the re-DHCP portal authentication mode, make sure the DHCP relay agent is enabled on the access device, and the DHCP server is installed and configured properly.
- The portal client, access device, and servers can reach each other.
- To use the remote RADIUS server, configure usernames and passwords on the RADIUS server, and configure the RADIUS client on the access device. For information about RADIUS client configuration, see "Configuring AAA."
- To implement extended portal functions, install and configure CAMS EAD or IMC EAD. Make sure the ACLs configured on the access device correspond to the isolation ACL and the security ACL on the security policy server. For information about security policy server configuration on the access device, see "Configuring AAA." For installation and configuration about the security policy server, see CAMS EAD Security Policy Component User Manual or IMC EAD Security Policy Help.
Configuring a portal authentication server

Perform this task to configure the following portal authentication server parameters:
• IP address of the portal authentication server
• VPN instance of the portal authentication server
• Shared encryption key used between the device and the portal authentication server
• Destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server

The device supports multiple portal authentication servers.

Do not delete a portal authentication server in use. Otherwise, users authenticated by that server cannot log out normally.

To configure a portal authentication server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>portal server server-name</code></td>
<td>By default, no portal authentication server is created.</td>
</tr>
</tbody>
</table>
| 3.   | - To specify an IPv4 portal server:  
        - To specify an IPv6 portal server:  
          - `ip ipv4-address [ vpn-instance vpn-instance-name ] [ key { cipher | simple } key-string ]`  
          - `ipv6 ipv6-address [ vpn-instance vpn-instance-name ] [ key { cipher | simple } key-string ]` | Specify an IPv4 portal authentication server, an IPv6 authentication portal server, or both.  
By default, no portal authentication server is specified. |
| 4.   | `port port-id` | By default, the UDP port number is 50100.  
This port number must be the same as the listening port number specified on the portal authentication server. |

Configuring a portal Web server

Perform this task to configure the following portal Web server parameters:
• VPN instance of the portal Web server
• URL of the portal Web server
• Parameters carried in the URL when the device redirects the URL to users

The device supports multiple portal Web servers.

To configure a portal Web server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>portal web-server server-name</code></td>
<td>By default, no portal Web server is created.</td>
</tr>
</tbody>
</table>
Enabling portal authentication on an interface

You must first enable portal authentication on an access interface before it can perform portal authentication for connected clients.

When a portal-enabled interface receives a portal packet, it checks the source IP address and VPN information of the packet. If the packet matches a locally configured portal authentication server, the interface regards the packet valid and sends an authentication response packet to the portal authentication server. Otherwise, the interface drops the packet. After a user logs in to the device, the user interacts with the portal authentication server as needed.

Configuration restrictions and guidelines

When you enable portal authentication on an interface, follow these restrictions and guidelines:

- Make sure the interface has a valid IP address before you enable re-DHCP portal authentication on the interface.
- Cross-subnet authentication mode (layer3) does not require Layer 3 forwarding devices between the access device and the portal authentication clients. However, if a Layer 3 forwarding device exists between the authentication client and the access device, you must use the cross-subnet portal authentication mode.
- With re-DHCP portal authentication, configure authorized ARP on the interface as a best practice to make sure only valid users can access the network. With authorized ARP configured on the interface, the interface learns ARP entries only from the users who have obtained a public address from DHCP.
- For successful re-DHCP portal authentication, make sure the BAS-IP/BAS-IPv6 attribute value is the same as the device IP or IPv6 address specified on the portal authentication server. To configure the BAS-IP/BAS-IPv6 attribute, use the portal { bas-ip | bas-ipv6 } command.
- An IPv6 portal server does not support the re-DHCP portal authentication mode.
- You can enable both IPv4 portal authentication and IPv6 portal authentication on an interface.

Configuration procedure

To enable portal authentication on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-number interface-type</td>
</tr>
<tr>
<td>3.</td>
<td>Enable portal authentication</td>
<td>• To enable IPv4 portal</td>
</tr>
</tbody>
</table>
Referencing a portal Web server for an interface

After you reference a portal Web server for an interface, the device redirects the HTTP requests of the portal users on the interface to the portal Web server.

An interface can reference both an IPv4 portal Web server and an IPv6 portal Web server.

To reference a portal Web server for an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
| 3.   | Reference a portal Web server for the interface. | • To reference an IPv4 portal Web server: portal apply web-server server-name [fail-permit]  
• To reference an IPv6 portal Web server: portal ipv6 apply web-server server-name [fail-permit] | Reference an IPv4 portal Web server, an IPv6 portal Web server, or both for the interface. By default, the interface does not reference any portal Web server. |

Controlling portal user access

Configuring a portal-free rule

A portal-free rule allows specified users to access specified external websites without portal authentication.

The matching items for a portal-free rule include the source/destination IP address, TCP/UDP port number, source MAC address, access interface, and VLAN. Packets matching a portal-free rule will not trigger portal authentication, so users sending the packets can directly access the specified external websites.

You cannot configure two or more portal-free rules with the same filtering criteria. Otherwise, the system prompts that the rule already exists.

Regardless of whether portal authentication is enabled or not, you can only add or remove a portal-free rule. You cannot modify it.

To configure an IP-based portal-free rule:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Configure an IPv4-based portal-free rule.</td>
<td>portal free-rule rule-number { destination ip { ip-address { mask-length</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an IPv6-based portal-free rule.</td>
<td>portal free-rule rule-number { destination ipv6 { ipv6-address prefix-length</td>
</tr>
</tbody>
</table>

To configure a source-based portal-free rule:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Configure source-based portal-free rule.</td>
<td>portal free-rule rule-number source { interface interface-type interface-number</td>
</tr>
</tbody>
</table>

### Configuring an authentication source subnet

By configuring authentication source subnets, you specify that only HTTP packets from users on the authentication source subnets can trigger portal authentication. If an unauthenticated user is not on any authentication source subnet, the access device discards all the user’s HTTP packets that do not match any portal-free rule.

When you configure a portal authentication source subnet, follow these restrictions and guidelines:

- Authentication source subnets apply only to cross-subnet portal authentication.
- In direct or re-DHCP portal authentication mode, a portal user and its access interface (portal-enabled) are on the same subnet. It is not necessary to specify the subnet as the authentication source subnet. If the specified authentication source subnet is different from the access subnet of the users, the users will fail the portal authentication.
  - In direct mode, the access device regards the authentication source subnet as any source IP address.
In re-DHCP mode, the access device regards the authentication source subnet on an interface as the subnet to which the private IP address of the interface belongs.

- If both authentication source subnets and destination subnets are configured on an interface, only the authentication destination subnets take effect.
- You can configure multiple authentication source subnets. If the source subnets overlap, the subnet with the largest address scope (with the smallest mask or prefix) takes effect.

To configure an IPv4 portal authentication source subnet:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>portal layer3 source ipv4-network-address { mask-length</td>
<td>mask }</td>
</tr>
</tbody>
</table>

To configure an IPv6 portal authentication source subnet:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>portal ipv6 layer3 source ipv6-network-address prefix-length</td>
<td>By default, no IPv6 portal authentication source subnet is configured, and IPv6 users from any subnets must pass portal authentication.</td>
</tr>
</tbody>
</table>

Configuring an authentication destination subnet

By configuring authentication destination subnets, you specify that users trigger portal authentication only when they accessing the specified subnets (excluding the destination IP addresses and subnets specified in portal-free rules). Users can access other subnets without portal authentication.

If both authentication source subnets and destination subnets are configured on an interface, only the authentication destination subnets take effect.

You can configure multiple authentication destination subnets. If the destination subnets overlap, the subnet with the largest address scope (with the smallest mask or prefix) takes effect.

To configure an IPv4 portal authentication destination subnet:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>portal free-all except destination ipv4-network-address { mask-length</td>
<td>mask }</td>
</tr>
</tbody>
</table>
To configure an IPv6 portal authentication destination subnet:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure an IPv6 portal authentication destination subnet.</td>
<td>portal ipv6 free-all except destination ipv6-network-address prefix-length</td>
</tr>
</tbody>
</table>

Setting the maximum number of portal users

Perform this task to control the total number of login IPv4 and IPv6 portal users in the system.

If the maximum number of portal users you set is less than that of the current login portal users, the limit can be set successfully and does not impact the login portal users. However, the system does not allow new portal users to log in until the number drops down below the limit.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the maximum number of portal users.</td>
<td>portal max-user max-number</td>
</tr>
</tbody>
</table>

Specifying a portal authentication domain

An authentication domain defines a set of authentication, authorization, and accounting policies. Each portal user belongs to an authentication domain and is authenticated, authorized, and accounted in the domain.

After you specify a portal authentication domain on an interface, the device uses the specified authentication domain for AAA of all portal users on the interface, ignoring the domain names carried in the usernames. This allows for flexible portal access control.

The device selects the authentication domain for a portal user on an interface in this order:

1. ISP domain specified for the interface.
2. ISP domain carried in the username.
3. System default ISP domain. For information about the default ISP domain, see “Configuring AAA.”

You can specify an IPv4 portal authentication domain, an IPv6 portal authentication domain, or both on an interface.

To specify an IPv4 portal authentication domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IPv4 portal</td>
<td>portal domain domain-name</td>
</tr>
</tbody>
</table>
To specify an IPv6 portal authentication domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an IPv6 portal authentication domain.</td>
<td>portal ipv6 domain domain-name</td>
</tr>
</tbody>
</table>

### Configuring portal detection features

#### Configuring online detection of portal users

Configure online detection to timely detect abnormal logouts of portal users.

- Configure ARP or ICMP detection for IPv4 portal users.
- Configure ND or ICMPv6 detection for IPv6 portal users.

If the device receives no packets from a portal user within the idle time, the device detects the user’s online status as follows:

- **ICMP or ICMPv6 detection**—Sends ICMP or ICMPv6 requests to the user at configurable intervals to detect the user status.
  - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.

- **ARP or ND detection**—Sends ARP or ND requests to the user and detects the ARP or ND entry status of the user at configurable intervals.
  - If the ARP or ND entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user’s ARP or ND entry. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the ARP or ND entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

ARP and ND detections apply only to direct and re-DHCP portal authentication. ICMP detection applies to all portal authentication modes.

To configure online detection of IPv4 portal users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure online</td>
<td>portal user-detect type { arp</td>
</tr>
</tbody>
</table>
To configure online detection of IPv6 portal users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure online detection of IPv6 portal users.</td>
<td>portal ipv6 user-detect type { icmpv6</td>
</tr>
</tbody>
</table>

By default, this feature is disabled on the interface.

### Configuring portal authentication server detection

During portal authentication, if the communication between the access device and portal authentication server is broken, both of the following occur:

- New portal users are not able to log in.
- The online portal users are not able to log out normally.

To address this problem, the access device needs to be able to detect the reachability changes of the portal server quickly and take corresponding actions to deal with the changes.

With the portal authentication server detection feature, the device periodically detects portal packets sent by a portal authentication server to determine the reachability of the server. If the device receives a portal packet within a detection timeout (timeout timeout) and the portal packet is valid, the device considers the portal authentication server to be reachable. Otherwise, the device considers the portal authentication server to be unreachable.

You can configure the device to take the following actions when the server reachability status changes:

- Sending a log message, which contains the name, the current state, and the original state of the portal authentication server.
- Enabling portal fail-permit. When the portal authentication server is unreachable, the portal fail-permit feature on an interface allows users on the interface to have network access. When the server recovers, it resumes portal authentication on the interface. For more information, see "Configuring the portal fail-permit feature."

Portal packets include user login packets, user logout packets, and heartbeat packets. Heartbeat packets are periodically sent by a server. By detecting heartbeat packets, the device can detect the server's actual status more quickly than by detecting other portal packets.

Only the IMC portal authentication server supports sending heartbeat packets. To test server reachability by detecting heartbeat packets, you must enable the server heartbeat feature on the IMC portal authentication server.

To configure portal authentication server detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter portal authentication server view.</td>
<td>portal server server-name</td>
</tr>
</tbody>
</table>

N/A
Configuring portal Web server detection

A portal authentication process cannot complete if the communication between the access device and the portal Web server is broken. To address this problem, you can enable portal Web server detection on the access device.

With the portal Web server detection feature, the access device simulates a Web access process to initiate a TCP connection to the portal Web server. If the TCP connection can be established successfully, the access device considers the detection successful, and the portal Web server is reachable. Otherwise, it considers the detection to have failed. Portal authentication status on interfaces of the access device does not affect the portal Web server detection feature.

You can configure the following detection parameters:

- **Detection interval**—Interval at which the device detects the server reachability.
- **Maximum number of consecutive failures**—If the number of consecutive detection failures reaches this value, the access device considers that the portal Web server is unreachable.

You can configure the device to take the following actions when the server reachability status changes:

- Sending a log message, which contains the name, the current state, and the original state of the portal Web server.
- Enabling portal fail-permit. When the portal Web server is unreachable, the portal fail-permit feature on an interface allows users on the interface to have network access. When the server recovers, it resumes portal authentication on the interface. For more information, see "Configuring the portal fail-permit feature."

To configure portal Web server detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter portal web-server</td>
<td>portal web-server server-name</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Configure portal Web</td>
<td>server-detect [ interval interval ] [ retry retries ] log</td>
<td>By default, portal Web server detection is disabled. This feature takes effect regardless of whether portal authentication is enabled on an interface or not.</td>
</tr>
</tbody>
</table>

Configuring portal user synchronization

Once the access device loses communication with a portal authentication server, the portal user information on the access device and that on the portal authentication server might be inconsistent after the communication resumes. To address this problem, the device provides the portal user synchronization feature. This feature is implemented by sending and detecting portal synchronization packets, as follows:
1. The portal authentication server sends the online user information to the access device in a synchronization packet at the user heartbeat interval, which is set on the portal authentication server.

2. Upon receiving the synchronization packet, the access device compares the users carried in the packet with its own user list. If a user contained in the packet does not exist on the access device, the access device informs the portal authentication server to delete the user. The access device starts the synchronization detection timer (timeout) immediately when a user logs in. If the user does not appear in any synchronization packet within a synchronization detection interval, the access device considers the user does not exist on the portal authentication server and logs the user out.

Portal user synchronization requires a portal authentication server to support the portal user heartbeat function. Only the IMC portal authentication server supports the portal user heartbeat function. To implement the portal user synchronization feature, you also need to configure the user heartbeat function on the portal authentication server. Make sure the user heartbeat interval configured on the portal authentication server is not greater than the synchronization detection timeout configured on the access device.

Deleting a portal authentication server on the access device also deletes the user synchronization configuration for the portal authentication server.

To configure portal user information synchronization:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter portal authentication server view.</td>
<td>portal server server-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure portal user synchronization.</td>
<td>user-sync timeout timeout</td>
</tr>
</tbody>
</table>

### Configuring the portal fail-permit feature

Perform this task to configure the portal fail-permit feature on an interface. When the access device detects that the portal authentication server or portal Web server is unreachable, it allows users on the interface to have network access without portal authentication.

If you enable fail-permit for both a portal authentication server and a portal Web server on an interface, the interface does the following:

- Disables portal authentication when either server is unreachable.
- Resumes portal authentication when both servers are reachable.

After portal authentication resumes, unauthenticated users must pass portal authentication to access the network. Users who have passed portal authentication before the fail-permit event can continue accessing the network.

To configure portal fail-permit:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---

### Configuring BAS-IP for portal packets sent to the portal authentication server

If the device runs Portal 2.0, the unsolicited packets sent to the portal authentication server must carry the BAS-IP attribute. If the device runs Portal 3.0, the unsolicited packets sent to the portal authentication server must carry the BAS-IP or BAS-IPv6 attribute.

If IPv4 portal authentication is enabled on an interface, you can configure the BAS-IP attribute on the interface. If IPv6 portal authentication is enabled on an interface, you can configure the BAS-IPv6 attribute on the interface.

After this attribute is configured, the source IP address for unsolicited notification portal packets the device sends to the portal authentication server is the configured BAS-IP or BAS-IPv6 address. If the attribute is not configured, the source IP address of the portal packets is the IP address of the packet output interface.

During a re-DHCP portal authentication or mandatory user logout process, the device sends portal notification packets to the portal authentication server. For the authentication or logout process to complete, make sure the BAS-IP/BAS-IPv6 attribute is the same as the device IP or IPv6 address specified on the portal authentication server.

To configure the BAS-IP attribute for portal packets sent to the portal authentication server on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 3. Configure BAS-IP for IPv4 portal packets sent to the portal authentication server. | portal bas-ip ipv4-address | By default:  
  • The BAS-IP attribute of an IPv4 portal reply packet sent to the portal authentication server is the source IPv4 address of the packet.  
  • The BAS-IP attribute of an IPv4 portal notification packet sent to the portal authentication server is the IPv4 address of the packet's output interface. |
| 4. Configure BAS-IPv6 for IPv6 portal packets sent to the portal authentication server. | portal bas-ipv6 ipv6-address | By default:  
  • The BAS-IPv6 attribute of an IPv6 portal reply packet sent to the portal authentication server is the source IPv6 address of the packet.  
  • The BAS-IPv6 attribute of an IPv6 portal notification packet sent to the portal authentication server is the IPv6 address of the packet's output interface. |
Applying a NAS-ID profile to an interface

By default, the device sends its device name in the NAS-Identifier attribute of any RADIUS requests. A NAS-ID profile enables you to send different NAS-Identifier attribute strings in RADIUS requests from different VLANs. The strings can be organization names, service names, or any user categorization criteria, depending on the administrative requirements.

For example, map the NAS-ID companyA to all VLANs of company A. The device will send companyA in the NAS-Identifier attribute for the RADIUS server to identify requests from any Company A users.

You can apply a NAS-ID profile to a portal-enabled interface. If no NAS-ID profile is specified on the interface or no matching NAS-ID is found in the specified profile, the device uses the device name as the interface NAS-ID.

To apply a NAS-ID profile to an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Create a NAS-ID profile and enter NAS-ID profile view.</td>
<td>aaa nas-id profile profile-name For more information about this command, see Security Commands Reference.</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a NAS ID and VLAN binding in the profile.</td>
<td>nas-id nas-identifier bind vlan vlan-id By default, no NAS ID and VLAN binding exists. For more information about this command, see Security Commands Reference.</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit N/A</td>
</tr>
<tr>
<td>5.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number N/A</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the NAS-ID profile on the interface.</td>
<td>portal profile-name nas-id-profile By default, no NAS-ID profile is specified on the interface.</td>
</tr>
</tbody>
</table>

Enabling portal roaming

Portal roaming takes effect only on portal users logging in from VLAN interfaces.

If portal roaming is enabled on a VLAN interface, an online portal user can access resources from any Layer 2 port in the VLAN without re-authentication.

If portal roaming is disabled, to access external network resources from a Layer 2 port different from the current access port in the VLAN, the user must do the following:

- First log out from the current port.
- Then re-authenticate on the new Layer 2 port.

To enable portal roaming:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enable portal roaming.</td>
<td>portal roaming enable By default, portal roaming is disabled. You cannot enable portal roaming when login users exist on the</td>
</tr>
</tbody>
</table>
### Logging out portal users

Logging out a user terminates the authentication process for the user or removes the user from the authenticated users list.

To log out users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Log out IPv4 portal users.</td>
<td>portal delete-user { ipv4-address</td>
</tr>
<tr>
<td>3.</td>
<td>Log out IPv6 portal users.</td>
<td>portal delete-user { all</td>
</tr>
</tbody>
</table>

### Configuring the local portal Web server feature

**IMPORTANT:**

This feature is available in Release 1121 and later.

To perform local portal authentication for users, perform the following tasks:

- Configure a local portal Web server.
- Configure a name for the portal Web server and specify a local IP address of the device as the server’s URL.
- Enable portal authentication on the user access interface.
- Specify the portal Web server on the portal-enabled interface.

During local portal authentication, the local Web portal server pushes authentication pages to users. You must customize the authentication pages and upload them to the device. On the device, specify an authentication page file as the default authentication page file for local portal authentication.

### Customizing authentication pages

Authentication pages are HTML files. Local portal authentication requires the following authentication pages:

- Logon page
- Logon success page
- Logon failure page
- Online page
- System busy page
- Logoff success page

You must customize the authentication pages, including the page elements that the authentication pages will use, for example, `back.jpg` for authentication page `Logon.htm`.

Follow the authentication page customization rules when you edit the authentication page files.
File name rules

The names of the main authentication page files are fixed (see Table 14). You can define the names of the files other than the main authentication page files. File names and directory names are case insensitive.

Table 14 Main authentication page file names

<table>
<thead>
<tr>
<th>Main authentication page</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon page</td>
<td>logon.htm</td>
</tr>
<tr>
<td>Logon success page</td>
<td>logonSuccess.htm</td>
</tr>
<tr>
<td>Logon failure page</td>
<td>logonFail.htm</td>
</tr>
<tr>
<td>Online page</td>
<td>online.htm</td>
</tr>
<tr>
<td>Pushed after the user gets online for online notification</td>
<td>busy.htm</td>
</tr>
<tr>
<td>System busy page</td>
<td></td>
</tr>
<tr>
<td>Pushed when the system is busy or the user is in the logon process</td>
<td>logoffSuccess.htm</td>
</tr>
</tbody>
</table>

Page request rules

The local portal Web server supports only Get and Post requests.

- **Get requests**—Used to get the static files in the authentication pages and allow no recursion. For example, if file Logon.htm includes contents that perform Get action on file ca.htm, file ca.htm cannot include any reference to file Logon.htm.
- **Post requests**—Used when users submit username and password pairs, log in, and log out.

Post request attribute rules

1. Observe the following requirements when editing a form of an authentication page:
   - An authentication page can have multiple forms, but there must be one and only one form whose action is logon.cgi. Otherwise, user information cannot be sent to the local portal Web server.
   - The username attribute is fixed as PtUser. The password attribute is fixed as PtPwd.
   - The value of the PtButton attribute is either Logon or Logoff, which indicates the action that the user requests.
   - A logon Post request must contain PtUser, PtPwd, and PtButton attributes.
   - A logoff Post request must contain the PtButton attribute.

2. Authentication pages logon.htm and logonFail.htm must contain the logon Post request. The following example shows part of the script in page logon.htm.
   ```html
   <form action=logon.cgi method = post >
   <p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px" maxlength=64>
   <p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px" maxlength=32>
   <p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;" onclick="form.action=form.action+location.search;"/>
   </form>
   ```

3. Authentication pages logonSuccess.htm and online.htm must contain the logoff Post request. The following example shows part of the script in page online.htm.
   ```html
   <form action=logon.cgi method = post >
   ```
Page file compression and saving rules

You must compress the authentication pages and their page elements into a standard zip file.

- The name of a zip file can contain only letters, numbers, and underscores.
- The authentication pages must be placed in the root directory of the zip file.
- Zip files can be transferred to the device through FTP or TFTP and must be saved in the root directory of the device.

Examples of zip files on the device:

```
<Sysname> dir
Directory of flash:
  1  -rw-  1405  Feb 28 2008 15:53:20
  0  -rw-  1405  Feb 28 2008 15:53:31
  2  -rw-  1405  Feb 28 2008 15:53:39
  3  -rw-  1405  Feb 28 2008 15:53:44
2540 KB total (1319 KB free)
```

Redirecting authenticated users to a specific webpage

To make the device automatically redirect authenticated users to a specific webpage, do the following in logon.htm and logonSuccess.htm:

1. In logon.htm, set the target attribute of Form to _blank.

   See the contents in gray:

   ```html
   <form method=post action=logon.cgi target="_blank">
   ```

2. Add the function for page loading pt_init() to logonSuccess.htm.

   See the contents in gray:

   ```html
   <html>
   <head>
   <title>LogonSuccessed</title>
   <script type="text/javascript" language="javascript" src="pt_private.js"></script>
   </head>
   <body onload="pt_init();" onbeforeunload="return pt_unload();">
   ... ...
   </body>
   </html>
   ```

Configuring a local portal Web server

Perform the following tasks for the local portal Web server to support HTTPS:

- Configure a PKI policy, obtain the CA certificate, and request a local certificate. For more information, see "Configuring PKI."
- Configure an SSL server policy, and specify the PKI domain configured in the PKI policy. For more information, see "Configuring SSL."

To configure a local portal Web server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2.</td>
<td>Create a local portal Web server and enter its view.</td>
<td>portal local-web-server { http</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the default authentication page file for the local portal Web server.</td>
<td>default-logon-page filename By default, no default authentication page file is specified for the local portal Web server.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Configure the listening TCP port for the local portal Web server.</td>
<td>tcp-port port-number By default, the HTTP service listening port number is 80 and the HTTPS service listening port number is the TCP port number set by the portal local-web-server command.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining portal

Execute `display` commands in any view and the `reset` command in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display portal rules on an interface.</td>
<td>display portal rule { all</td>
</tr>
<tr>
<td>Display portal configuration and portal running state information on an interface.</td>
<td>display portal interface interface-type interface-number</td>
</tr>
<tr>
<td>Display portal authentication server information.</td>
<td>display portal server [ server-name ]</td>
</tr>
<tr>
<td>Display portal Web server information.</td>
<td>display portal web-server [ server-name ]</td>
</tr>
<tr>
<td>Display packet statistics for portal authentication servers.</td>
<td>display portal packet statistics [ server server-name ]</td>
</tr>
<tr>
<td>Display portal user information.</td>
<td>display portal user { all</td>
</tr>
<tr>
<td>Clear packet statistics for portal authentication servers.</td>
<td>reset portal packet statistics [ server server-name ]</td>
</tr>
</tbody>
</table>

## Portal configuration examples

### Configuring direct portal authentication

#### Network requirements

As shown in Figure 42, the host is directly connected to the switch (the access device). The host is assigned with a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication, so the host can access only the portal server before passing the authentication and access other network resources after passing the authentication.
Configuration prerequisites

- Configure IP addresses for the host, switch, and servers as shown in Figure 42 and make sure they can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.

Configuring the portal authentication server on IMC PLAT 3.20

This example assumes that the portal server runs on IMC PLAT 3.20-R2602P13 and IMC UAM 3.60-E6301.

1. Configure the portal authentication server:
   a. Log in to IMC and click the Service tab.
   b. Select Access Service > Portal Service Management > Server from the navigation tree to enter the portal server configuration page, as shown in Figure 43.
   c. Configure the portal server parameters as needed. This example uses the default values.
   d. Click OK.

Figure 43 Portal authentication server configuration

2. Configure the IP address group:
   a. Select Access Service > Portal Service Management > IP Group from the navigation tree to enter the portal IP address group configuration page.
   b. Click Add to enter the page shown in Figure 44.
   c. Enter the IP group name.
   d. Enter the start IP address and end IP address of the IP group. Make sure the host IP address (2.2.2.2) is in the IP group.
e. Select a service group. 
   This example uses the default group **Ungrouped**.

f. Select **Normal** from the **Action** list.

g. Click **OK**.

**Figure 44 Adding an IP address group**

3. Add a portal device:
   a. Select **Access Service > Portal Service Management > Device** from the navigation tree to enter the portal device configuration page.
   b. Click **Add** to enter the page shown in **Figure 45**.
   c. Enter the device name **NAS**.
   d. Enter the IP address of the switch’s interface connected to the host.
   e. Enter the key, which must be the same as that configured on the switch.
   f. Set whether to enable IP address reallocation.
      This example uses direct portal authentication, and therefore select **No** from the Reallocate IP list.
   g. Set whether to support the portal server heartbeat and user heartbeat functions.
      In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
   h. Click **OK**.

**Figure 45 Adding a portal device**

4. Associate the portal device with the IP address group:
a. As shown in Figure 46, click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.

**Figure 46 Device list**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Version</th>
<th>Service Group</th>
<th>IP Address</th>
<th>Details</th>
<th>Modify</th>
<th>Port Group Information Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS</td>
<td>Portal 2.0</td>
<td>Ungrouped</td>
<td>2.2.2.1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

b. Click **Add** to enter the page shown in Figure 47.

**Figure 47 Port group configuration**

- **Port Group Information**
  - **Port Group Name**: group
  - **Start Port**: 0
  - **Protocol**: HTTP
  - **NAT or Not**: NO
  - **Authentication Type**: CHAP
  - **Heartbeat Interval**: 10
  - **Language**: Dynamic Detection
  - **End Port**: zzzzzzz
  - **Quick Authentication**: No
  - **Enter Transparent Transmission**: Yes
  - **IP Group**: Portal_user
  - **Heartbeat Timeout**: 30
  - **Port Group Description**:
  - **Default Authentication Page**: index_default.jsp

- **User Domain**
- **User Attribute Type**
- **Default Authentication Type**

- **OK**
- **Cancel**

c. Enter the port group name.
d. Select the configured IP address group.
The IP address used by the user to access the network must be within this IP address group.
e. Click **OK**.

5. Select **Access Service > Service Parameters > Validate System Configuration** from the navigation tree to validate the configurations.

**Configuring the portal authentication server on IMC PLAT 5.0**

This example assumes that the portal server runs on IMC PLAT 5.0(E0101) and IMC UAM 5.0(E0101).

1. Configure the portal authentication server:
   a. Log in to IMC and click the **Service** tab.
   b. Select **User Access Manager > Portal Service Management > Server** from the navigation tree to enter the portal server configuration page, as shown in Figure 48.
   c. Configure the portal server parameters as needed.
      This example uses the default settings.
d. Click **OK**.
2. Configure the IP address group:
   a. Select User Access Manager > Portal Service Management > IP Group from the navigation tree to enter the portal IP address group configuration page.
   b. Click Add to enter the page shown in Figure 49.
   c. Enter the IP group name.
   d. Enter the start IP address and end IP address of the IP group. Make sure the host IP address is in the IP group.
   e. Select a service group.
      This example uses the default group Ungrouped.
   f. Select Normal from the Action list.
   g. Click OK.

Figure 49 Adding an IP address group

3. Add a portal device:
a. Select **User Access Manager > Portal Service Management > Device** from the navigation tree to enter the portal device configuration page.
b. Click **Add** to enter the page shown in Figure 50.
c. Enter the device name **NAS**.
d. Enter the IP address of the switch’s interface connected to the host.
e. Enter the key, which must be the same as that configured on the switch.
f. Set whether to enable IP address reallocation.
   - This example uses direct portal authentication, and therefore select **No** from the **Reallocate IP** list.
g. Select whether to support server heartbeat and user heartbeat functions.
   - In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
h. Click **OK**.

**Figure 50 Adding a portal device**

4. Associate the portal device with the IP address group:
   a. As shown in Figure 51, click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.
b. Click **Add** to enter the page shown in Figure 52.
c. Enter the port group name.
d. Select the configured IP address group.
   - The IP address used by the user to access the network must be within this IP address group.
e. Use the default settings for other parameters.
f. Click **OK**.

**Figure 51 Device list**
5. Select User Access Manager > Service Parameters > Validate System Configuration from the navigation tree to validate the configurations.

Configuring the switch

1. Configure a RADIUS scheme:

   # Create a RADIUS scheme named rs1 and enter its view.
   
   ```
   <Switch> system-view
   [Switch] radius scheme rs1
   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
   [Switch-radius-rs1] primary authentication 192.168.0.112
   [Switch-radius-rs1] primary accounting 192.168.0.112
   [Switch-radius-rs1] key authentication simple radius
   [Switch-radius-rs1] key accounting simple radius
   # Exclude the ISP domain name from the username sent to the RADIUS server.
   [Switch-radius-rs1] user-name-format without-domain
   [Switch-radius-rs1] quit
   # Enable RADIUS session control.
   [Switch] radius session-control enable
   ```

2. Configure an authentication domain:

   # Create an ISP domain named dm1 and enter its view.
   ```
   [Switch] domain dm1
   # Configure AAA methods for the ISP domain.
   [Switch-isp-dm1] authentication portal radius-scheme rs1
   [Switch-isp-dm1] authorization portal radius-scheme rs1
   [Switch-isp-dm1] accounting portal radius-scheme rs1
   [Switch-isp-dm1] quit
   # Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
   [Switch] domain default enable dm1
   ```

3. Configure portal authentication:
# Configure a portal authentication server.
[Switch] portal server newpt
New portal server added.
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100
[Switch-portal-server-newpt] quit

# Configure a portal Web server.
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] quit

# Enable direct portal authentication on VLAN-interface 100.
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method direct

# Reference the portal Web server newpt on VLAN-interface 100.
[Switch-Vlan-interface100] portal apply web-server newpt

# Configure the BAS-IP as 2.2.2.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.
[Switch-Vlan-interface100] portal bas-ip 2.2.2.1
[Switch-Vlan-interface100] quit

Verifying the configuration

# Verify that the portal configuration has taken effect.
[Switch] display portal interface vlan-interface 100
Portal information of Vlan-interface100
  Nas id profile: Not configured
IPv4:
  Portal status: Enabled
  Authentication type: Direct
  Portal Web server: newpt
  Authentication domain: Not configured
  Bas-ip: 2.2.2.1
  User Detection: Not configured
  Action for server detection:
    Server type Server name Action
    -- -- --
  Layer3 source network:
    IP address Mask
  Destination authenticate subnet:
    IP address Mask
IPv6:
  Portal status: Disabled
  Authentication type: Disabled
  Portal Web server: Not configured
  Authentication domain: Not configured
  Bas-ipv6: Not configured
  User detection: Not configured
  Action for server detection:
    Server type Server name Action
A user can perform portal authentication by using the HPE iNode client or a Web browser. Before passing the authentication, the user can access only the authentication page http://192.168.0.111:8080/portal and all Web requests will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

# After the user passes authentication, use the following command to display information about the portal user.

```
[Switch] display portal user interface vlan-interface 100
```

Total portal users: 1
Username: abc
Portal server: newpt
State: Online
Authorization ACL: --
VPN instance: --

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0015-e9a6-7cfe</td>
<td>2.2.2.2</td>
<td>100</td>
<td>Vlan-interface100</td>
</tr>
</tbody>
</table>

### Configuring re-DHCP portal authentication

**Network requirements**

As shown in Figure 53, the host is directly connected to the switch (the access device). The host obtains an IP address through the DHCP server. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure re-DHCP portal authentication. Before passing the authentication, the host is assigned a private IP address. After passing the authentication, the host gets a public IP address and can access Internet resources.

**Figure 53 Network diagram**
Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 53 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
- For re-DHCP portal authentication, configure a public address pool (20.20.20.0/24) and a private address pool (10.0.0.0/24) on the DHCP server. (Details not shown.)
- For re-DHCP portal authentication:
  - The switch must be configured as a DHCP relay agent.
  - The portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).

For information about DHCP relay agent configuration, see Layer 3—IP Services Configuration Guide.

- Make sure the IP address of the portal device added on the portal server is the public IP address (20.20.20.1) of the switch's interface connecting the host. The private IP address range for the IP address group associated with the portal device is the private subnet 10.0.0.0/24 where the host resides. The public IP address range for the IP address group is the public subnet 20.20.20.0/24.

Configuration procedure

Perform the following tasks on the switch.

1. Configure a RADIUS scheme:

   # Create a RADIUS scheme named rs1 and enter its view.
   <Switch> system-view
   [Switch] radius scheme rs1
   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
   [Switch-radius-rs1] primary authentication 192.168.0.113
   [Switch-radius-rs1] primary accounting 192.168.0.113
   [Switch-radius-rs1] key authentication simple radius
   [Switch-radius-rs1] key accounting simple radius
   # Exclude the ISP domain name from the username sent to the RADIUS server.
   [Switch-radius-rs1] user-name-format without-domain
   [Switch-radius-rs1] quit
   # Enable RADIUS session control.
   [Switch] radius session-control enable

2. Configure an authentication domain:

   # Create an ISP domain named dm1 and enter its view.
   [Switch] domain dm1
   # Configure AAA methods for the ISP domain.
   [Switch-isp-dm1] authentication portal radius-scheme rs1
   [Switch-isp-dm1] authorization portal radius-scheme rs1
   [Switch-isp-dm1] accounting portal radius-scheme rs1
   [Switch-isp-dm1] quit
   # Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
   [Switch] domain default enable dm1

3. Configure DHCP relay and authorized ARP:
# Configure DHCP relay.
[Switch] dhcp enable
[Switch] dhcp relay client-information record
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 20.20.20.1 255.255.255.0
[Switch-Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
[Switch-Vlan-interface100] dhcp select relay
[Switch-Vlan-interface100] dhcp relay server-address 192.168.0.112
# Enable authorized ARP.
[Switch-Vlan-interface100] arp authorized enable
[Switch-Vlan-interface100] quit

4. Configure portal authentication:
# Configure a portal authentication server.
[Switch] portal server newpt
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100
[Switch-portal-server-newpt] quit

# Configure a portal Web server.
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] quit

# Enable re-DHCP portal authentication on VLAN-interface 100.
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method redhcp

# Reference the portal Web server newpt on VLAN-interface 100.
[Switch-Vlan-interface100] portal apply web-server newpt

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.
[Switch-Vlan-interface100] portal bas-ip 20.20.20.1
[Switch-Vlan-interface100] quit

Verifying the configuration

# Verify that the portal configuration has taken effect.
[Switch] display portal interface vlan-interface 100
Portal information of Vlan-interface100
  Nas id profile: Not configured
IPv4:
  Portal status: Enabled
  Authentication type: Redhcp
  Portal Web server: newpt
  Authentication domain: Not configured
  Bas-ip: 20.20.20.1
  User Detection: Not configured
  Action for server detection:

        Server type    Server name    Action
  ---    ---    ---

Layer3 source network:

  IP address    Mask
A user can perform portal authentication by using the HPE iNode client or a Web browser. Before passing the authentication, the user can access only the authentication page \url{http://192.168.0.111:8080/portal} and all Web requests will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

# After the user passes authentication, use the following command to display information about the portal user.

```sh
[Switch] display portal user interface vlan-interface 100
```

Total portal users: 1
Username: abc
Portal server: newpt
State: Online
Authorization ACL: None
VPN instance: --

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0015-e9a6-7cfe</td>
<td>20.20.20.2</td>
<td>100</td>
<td>Vlan-interface100</td>
</tr>
</tbody>
</table>

### Configuring cross-subnet portal authentication

#### Network requirements

As shown in Figure 54, Switch A supports portal authentication. The host accesses Switch A through Switch B. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure Switch A for cross-subnet portal authentication. Before passing the authentication, the host can access only the portal Web server. After passing the authentication, the user can access Internet resources.
Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 54 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
- Make sure the IP address of the portal device added on the portal authentication server is the IP address (20.20.20.1) of the switch’s interface connecting the host. The IP address group associated with the portal device is the subnet of the host (8.8.8.0/24).

Configuration procedure

Perform the following tasks on Switch A.

1. Configure a RADIUS scheme:

   ```
   # Create a RADIUS scheme named rs1 and enter its view.
   <SwitchA> system-view
   [SwitchA] radius scheme rs1
   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
   [SwitchA-radius-rs1] primary authentication 192.168.0.112
   [SwitchA-radius-rs1] primary accounting 192.168.0.112
   [SwitchA-radius-rs1] key authentication simple radius
   [SwitchA-radius-rs1] key accounting simple radius
   # Exclude the ISP domain name from the username sent to the RADIUS server.
   [SwitchA-radius-rs1] user-name-format without-domain
   [SwitchA-radius-rs1] quit
   # Enable RADIUS session control.
   [SwitchA] radius session-control enable
   ```

2. Configure an authentication domain:

   ```
   # Create an ISP domain named dm1 and enter its view.
   [SwitchA] domain dm1
   # Configure AAA methods for the ISP domain.
   [SwitchA-isp-dm1] authentication portal radius-scheme rs1
   [SwitchA-isp-dm1] authorization portal radius-scheme rs1
   [SwitchA-isp-dm1] accounting portal radius-scheme rs1
   [SwitchA-isp-dm1] quit
   ```
# Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

[SwitchA] domain default enable dm1

3. Configure portal authentication:

# Configure a portal authentication server.

[SwitchA] portal server newpt
[SwitchA-portal-server-newpt] ip 192.168.0.111 key simple portal
[SwitchA-portal-server-newpt] port 50100
[SwitchA-portal-server-newpt] quit

# Configure a portal Web server.

[SwitchA] portal web-server newpt
[SwitchA-portal-websvr-newpt] quit

# Enable cross-subnet portal authentication on VLAN-interface 4.

[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] portal enable method layer3

# Reference the portal Web server newpt on VLAN-interface 4.

[SwitchA-Vlan-interface4] portal apply web-server newpt

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from VLAN-interface 4 to the portal authentication server.

[SwitchA-Vlan-interface4] portal bas-ip 20.20.20.1
[SwitchA-Vlan-interface4] quit

On Switch B, configure a default route to subnet 192.168.0.0/24, specifying the next hop address as 20.20.20.1. (Details not shown.)

Verifying the configuration

# Verify that the portal configuration has taken effect.

[SwitchA] display portal interface vlan-interface 4

PORTAL information of Vlan-interface4
Nas id profile: Not configured
IPv4:
 Portal status: Enabled
 Authentication type: Layer3
 Portal Web server: newpt
 Authentication domain: Not configured
 Bas-ip: 20.20.20.1
 User Detection: Not configured
 Action for server detection:

<table>
<thead>
<tr>
<th>Server type</th>
<th>Server name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

Layer3 source network:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Mask</th>
</tr>
</thead>
</table>

Destination authenticate subnet:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Mask</th>
</tr>
</thead>
</table>

IPv6:

Portal status: Disabled
Authentication type: Disabled
Portal Web server: Not configured
Authentication domain: Not configured
Bas-ipv6: Not configured
User detection: Not configured

Action for server detection:

<table>
<thead>
<tr>
<th>Server type</th>
<th>Server name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Layer3 source network:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Prefix length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Destination authenticate subnet:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Prefix length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A user can perform portal authentication by using the HPE iNode client or a Web browser. Before passing the authentication, the user can access only the authentication page http://192.168.0.111:8080/portal and all Web requests will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

# After the user passes authentication, use the following command to display information about the portal user.

[SwitchA] display portal user interface vlan-interface 4

Total portal users: 1
Username: abc
Portal server: newpt
State: Online
Authorization ACL: None
VPN instance: --

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0015-e9a6-7cfe</td>
<td>8.8.8.2</td>
<td>4</td>
<td>Vlan-interface4</td>
</tr>
</tbody>
</table>

Configuring extended direct portal authentication

Network requirements

As shown in Figure 55, the host is directly connected to the switch (the access device). The host is assigned with a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure extended direct portal authentication. If the host fails security check after passing identity authentication, it can access only subnet 192.168.0.0/24. After passing security check, the host can access Internet resources.
Configuration prerequisites

- Configure IP addresses for the host, switch, and servers as shown in Figure 55 and make sure they can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.

Configuration procedure

Perform the following tasks on the switch.

1. Configure a RADIUS scheme:
   
   # Create a RADIUS scheme named rs1 and enter its view.
   
   ```
   <Switch> system-view
   [Switch] radius scheme rs1
   ```
   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
   
   ```
   [Switch-radius-rs1] primary authentication 192.168.0.112
   [Switch-radius-rs1] primary accounting 192.168.0.112
   [Switch-radius-rs1] key accounting simple radius
   [Switch-radius-rs1] key authentication simple radius
   [Switch-radius-rs1] user-name-format without-domain
   ```
   # Specify the security policy server.
   
   ```
   [Switch-radius-rs1] security-policy-server 192.168.0.113
   ```
   # Enable RADIUS session control.
   
   ```
   [Switch] radius session-control enable
   ```

2. Configure an authentication domain:
   
   # Create an ISP domain named dm1 and enter its view.
   
   ```
   [Switch] domain dm1
   ```
   # Configure AAA methods for the ISP domain.
   
   ```
   [Switch-isp-dm1] authentication portal radius-scheme rs1
   [Switch-isp-dm1] authorization portal radius-scheme rs1
   [Switch-isp-dm1] accounting portal radius-scheme rs1
   ```
   # Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL:

```bash
[Switch] domain default enable dm1

[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Switch-acl-adv-3000] rule deny ip
[Switch-acl-adv-3000] quit

[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip
[Switch-acl-adv-3001] quit
```

**NOTE:**
Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

4. Configure portal authentication:

```bash
# Configure a portal authentication server.
[Switch] portal server newpt
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100
[Switch-portal-server-newpt] quit

# Configure a portal Web server.
[Switch] portal web-server newpt
[Switch-portal-webserver-newpt] quit

# Enable direct portal authentication on VLAN-interface 100.
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method direct

# Reference the portal Web server newpt on VLAN-interface 100.
[Switch-Vlan-interface100] portal apply web-server newpt

# Configure the BAS-IP as 2.2.2.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.
[Switch-Vlan-interface100] portal bas-ip 2.2.2.1
[Switch-Vlan-interface100] quit
```

**Verifying the configuration**

```bash
# Verify that the portal configuration has taken effect.
[Switch] display portal interface vlan-interface 100

Portal information of Vlan-interface100
Nas id profile: Not configured
IPv4:
  Portal status: Enabled
  Authentication type: Direct
  Portal Web server: newpt
  Authentication domain: Not configured
  Bas-ip: 2.2.2.1
  User Detection: Not configured
  Action for server detection:
    Server type Server name Action
    --     --      --
```
Layer3 source network:
  IP address                  Mask

Destination authenticate subnet:
  IP address                  Mask

IPv6:
  Portal status: Disabled
  Authentication type: Disabled
  Portal Web server: Not configured
  Authentication domain: Not configured
  Bas-ipv6: Not configured
  User detection: Not configured

Action for server detection:
  Server type    Server name                        Action
  --             --                                 --

Layer3 source network:
  IP address                  Prefix length

Destination authenticate subnet:
  IP address                  Prefix length

Before a user performs portal authentication by using the HPE iNode client, the user can access only the authentication page [http://192.168.0.111:8080/portal](http://192.168.0.111:8080/portal). All Web requests the user initiates will be redirected to the authentication page.

- If the user passes the authentication but fails the security check, the user can access only the resources that match ACL 3000.
- After passing both the authentication and the security check, the user can access Internet resources that match ACL 3001.

# After the user passes authentication, use the following command to display information about the portal user.

```
[Switch] display portal user interface vlan-interface 100
```

Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
  VPN instance: --

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0015-e9a6-7cfe</td>
<td>2.2.2.2</td>
<td>100</td>
<td>Vlan-interface100</td>
</tr>
</tbody>
</table>

Configuring extended re-DHCP portal authentication

Network requirements

As shown in Figure 56, the host is directly connected to the switch (the access device). The host obtains an IP address through the DHCP server. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure extended re-DHCP portal authentication. Before passing portal authentication, the host is assigned a private IP address. After passing portal identity authentication, the host obtains a public IP address and accepts security check. If the host fails the security check, it can access only subnet 192.168.0.0/24. After passing the security check, the host can access Internet resources.
Figure 56 Network diagram

Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 56 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
- For re-DHCP portal authentication, configure a public address pool (20.20.0.0/24) and a private address pool (10.0.0.0/24) on the DHCP server. (Details not shown.)
- For re-DHCP portal authentication:
  - The switch must be configured as a DHCP relay agent.
  - The portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).
  For information about DHCP relay agent configuration, see Layer 3—IP Services Configuration Guide.
- Make sure the IP address of the portal device added on the portal server is the public IP address (20.20.0.1) of the switch’s interface connecting the host. The private IP address range for the IP address group associated with the portal device is the private subnet 10.0.0.0/24 where the host resides. The public IP address range for the IP address group is the public subnet 20.20.0.0/24.

Configuration procedure

Perform the following tasks on the switch.

1. Configure a RADIUS scheme:
   
   # Create a RADIUS scheme named rs1 and enter its view.
   <Switch> system-view
   [Switch] radius scheme rs1
   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
   [Switch-radius-rs1] primary authentication 192.168.0.113
   [Switch-radius-rs1] primary accounting 192.168.0.113
   [Switch-radius-rs1] key accounting simple radius
   [Switch-radius-rs1] key authentication simple radius
   [Switch-radius-rs1] user-name-format without-domain
   # Specify the security policy server.
2. Configure an authentication domain:
   # Create an ISP domain named dm1 and enter its view.
   [Switch] domain dm1
   # Configure AAA methods for the ISP domain.
   [Switch-isp-dm1] authentication portal radius-scheme rs1
   [Switch-isp-dm1] authorization portal radius-scheme rs1
   [Switch-isp-dm1] accounting portal radius-scheme rs1
   [Switch-isp-dm1] quit
   # Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
   [Switch] domain default enable dm1

3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL:
   [Switch] acl number 3000
   [Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
   [Switch-acl-adv-3000] rule deny ip
   [Switch-acl-adv-3000] quit
   [Switch] acl number 3001
   [Switch-acl-adv-3001] rule permit ip
   [Switch-acl-adv-3001] quit

   NOTE:
   Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

4. Configure DHCP relay and authorized ARP:
   # Configure DHCP relay.
   [Switch] dhcp enable
   [Switch] dhcp relay client-information record
   [Switch] interface vlan-interface 100
   [Switch-Vlan-interface100] ip address 20.20.20.1 255.255.255.0
   [Switch-Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
   [Switch-Vlan-interface100] dhcp select relay
   [Switch-Vlan-interface100] dhcp relay server-address 192.168.0.112
   # Enable authorized ARP.
   [Switch-Vlan-interface100] arp authorized enable
   [Switch-Vlan-interface100] quit

5. Configure portal authentication:
   # Configure a portal authentication server.
   [Switch] portal server newpt
   [Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
   [Switch-portal-server-newpt] port 50100
   [Switch-portal-server-newpt] quit
   # Configure a portal Web server.
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] quit

# Enable re-DHCP portal authentication on VLAN-interface 100.
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method redhcp

# Reference the portal Web server newpt on VLAN-interface 100.
[Switch-Vlan-interface100] portal apply web-server newpt

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.
[Switch-Vlan-interface100] portal bas-ip 20.20.20.1
[Switch-Vlan-interface100] quit

Verifying the configuration

# Verify that the portal configuration has taken effect.
[Switch] display portal interface vlan-interface 100

Portal information of Vlan-interface100
  Nas id profile: Not configured
IPv4:
  Portal status: Enabled
  Authentication type: Redhcp
  Portal Web server: newpt
  Authentication domain: Not configured
  Bas-ip: 20.20.20.1
  User Detection: Not configured
  Action for server detection:
    Server type    Server name                        Action
      --             --                                 --
  Layer3 source network:
    IP address               Mask

  Destination authenticate subnet:
    IP address               Mask
IPv6:
  Portal status: Disabled
  Authentication type: Disabled
  Portal Web server: Not configured
  Authentication domain: Not configured
  Bas-ipv6: Not configured
  User detection: Not configured
  Action for server detection:
    Server type    Server name                        Action
      --             --                                 --
  Layer3 source network:
    IP address               Prefix length

  Destination authenticate subnet:
    IP address               Prefix length
Before a user performs portal authentication by using the HPE iNode client, the user can access only the authentication page http://192.168.0.111:8080/portal. All Web requests the user initiates will be redirected to the authentication page.

- If the user passes the authentication but fails the security check, the user can access only the resources that match ACL 3000.
- After passing both the authentication and the security check, the user can access Internet resources that match ACL 3001.

# After the user passes authentication, use the following command to display information about the portal user.

```bash
[Switch] display portal user interface vlan-interface 100
```

Total portal users: 1

Username: abc

- Portal server: newpt
- State: Online
- Authorization ACL: 3001
- VPN instance: --

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0015-e9a6-7cfe</td>
<td>20.20.20.2</td>
<td>100</td>
<td>Vlan-interface100</td>
</tr>
</tbody>
</table>

Configuring extended cross-subnet portal authentication

Network requirements

As shown in Figure 57, Switch A supports portal authentication. The host accesses Switch A through Switch B. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure Switch A for extended cross-subnet portal authentication. Before passing portal authentication, the host can access only the portal server. After passing portal identity authentication, the host accepts security check. If the host fails the security check it can access only the subnet 192.168.0.0/24. After passing the security check, the host can access Internet resources.

Figure 57 Network diagram

Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 57 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
• Make sure the IP address of the portal device added on the portal server is the IP address (20.20.20.1) of the switch's interface connecting the host. The IP address group associated with the portal device is the subnet of the host (8.8.8.0/24).

Configuration procedure

Perform the following tasks on Switch A.

1. Configure a RADIUS scheme:
   # Create a RADIUS scheme named **rs1** and enter its view.
   
   ```
   <SwitchA> system-view
   [SwitchA] radius scheme rs1
   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
   [SwitchA-radius-rs1] primary authentication 192.168.0.112
   [SwitchA-radius-rs1] primary accounting 192.168.0.112
   [SwitchA-radius-rs1] key accounting simple radius
   [SwitchA-radius-rs1] key authentication simple radius
   [SwitchA-radius-rs1] user-name-format without-domain
   # Specify the security policy server.
   [SwitchA-radius-rs1] security-policy-server 192.168.0.113
   [SwitchA-radius-rs1] quit
   # Enable RADIUS session control.
   [SwitchA] radius session-control enable
   ```

2. Configure an authentication domain:
   # Create an ISP domain named **dm1** and enter its view.
   
   ```
   [SwitchA] domain dm1
   # Configure AAA methods for the ISP domain.
   [SwitchA-isp-dm1] authentication portal radius-scheme rs1
   [SwitchA-isp-dm1] authorization portal radius-scheme rs1
   [SwitchA-isp-dm1] accounting portal radius-scheme rs1
   [SwitchA-isp-dm1] quit
   # Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
   [SwitchA] domain default enable dm1
   ```

3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL:
   
   ```
   [SwitchA] acl number 3000
   [SwitchA-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
   [SwitchA-acl-adv-3000] rule deny ip
   [SwitchA-acl-adv-3000] quit
   [SwitchA] acl number 3001
   [SwitchA-acl-adv-3001] rule permit ip
   [SwitchA-acl-adv-3001] quit
   ```

   **NOTE:**
   Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

4. Configure portal authentication:
   # Configure a portal authentication server.
[SwitchA] portal server newpt
[SwitchA-portal-server-newpt] ip 192.168.0.111 key simple portal
[SwitchA-portal-server-newpt] port 50100
[SwitchA-portal-server-newpt] quit

# Configure a portal Web server.
[SwitchA] portal web-server newpt
[SwitchA-portal-websvr-newpt] quit

# Enable cross-subnet portal authentication on VLAN-interface 4.
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] portal enable method layer3

# Reference the portal Web server newpt on VLAN-interface 4.
[SwitchA-Vlan-interface4] portal apply web-server newpt

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from VLAN-interface 4 to the portal authentication server.
[SwitchA-Vlan-interface4] portal bas-ip 20.20.20.1
[SwitchA-Vlan-interface4] quit

On Switch B, configure a default route to subnet 192.168.0.0/24, specifying the next hop address as 20.20.20.1. (Details not shown.)

Verifying the configuration

# Verify that the portal configuration has taken effect.
[SwitchA] display portal interface vlan-interface 4
Portal information of Vlan-interface4
  Nas id profile: Not configured
IPv4:
  Portal status: Enabled
  Authentication type: Layer3
  Portal Web server: newpt
  Authentication domain: Not configured
  Bas-ip: 20.20.20.1
  User Detection: Not configured
  Action for server detection:
    Server type    Server name                        Action
    --             --                                 --
  Layer3 source network:
    IP address               Mask

  Destination authenticate subnet:
    IP address               Mask
IPv6:
  Portal status: Disabled
  Authentication type: Disabled
  Portal Web server: Not configured
  Authentication domain: Not configured
  Bas-ipv6: Not configured
  User detection: Not configured
  Action for server detection:
    Server type    Server name                        Action
    --             --                                 --
Before a user performs portal authentication by using the HPE iNode client, the user can access only the authentication page http://192.168.0.111:8080/portal. All Web requests the user initiates will be redirected to the authentication page.

- If the user passes the authentication but fails the security check, the user can access only the resources that match ACL 3000.
- After passing both the authentication and the security check, the user can access Internet resources that match ACL 3001.

# After the user passes authentication, use the following command to display information about the portal user.

```
[SwitchA] display portal user interface vlan-interface 4
```

Total portal users: 1
Username: abc
Portal server: newpt
State: Online
Authorization ACL: 3001
VPN instance: --

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0015-e9a6-7cfe</td>
<td>8.8.8.2</td>
<td>4</td>
<td>Vlan-interface4</td>
</tr>
</tbody>
</table>

Configuring portal server detection and portal user synchronization

Network requirements

As shown in Figure 58, the host is directly connected to the switch (the access device). The host is assigned with a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication on the switch, so the host can access only the portal server before passing the authentication and access Internet resources after passing the authentication.

Configure the switch to do the following:

- Detect the reachability state of the portal authentication server.
- Send log messages upon state changes.
- Disable portal authentication when the authentication server is unreachable.
- Synchronize portal user information with the portal server periodically.
Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 58 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
- Configure the portal authentication server. Be sure to enable the server heartbeat function and the user heartbeat function.
- Configure the switch (access device) as follows:
  - Configure direct portal authentication on VLAN-interface 100, the interface to which the host is connected.
  - Configure portal authentication server detection, so that the switch can detect the reachability of the portal authentication server by cooperating with the portal server heartbeat function.
  - Configure portal user synchronization, so that the switch can synchronize portal user information with the portal authentication server by cooperating with the portal user heartbeat function.

Configuring the portal authentication server on IMC PLAT 3.20

This example assumes that the portal server runs on IMC PLAT 3.20-R2602P13 and IMC UAM 3.60-E6301.

1. Configure the portal authentication server:
   a. Log in to IMC and click the Service tab.
   b. Select Access Service > Portal Service Management > Server from the navigation tree to enter the portal server configuration page, as shown in Figure 59.
   c. Configure the portal server heartbeat interval and user heartbeat interval.
   d. Use the default settings for other parameters.
   e. Click OK.
2. Configure the IP address group:
   a. Select **Access Service > Portal Service Management > IP Group** from the navigation tree to enter the portal IP address group configuration page.
   b. Click **Add** to enter the page shown in **Figure 60**.
   c. Enter the IP group name.
   d. Enter the start IP address and end IP address of the IP group.
      Make sure the host IP address (2.2.2.2) is in the IP group.
   e. Select a service group.
      This example uses the default group *Ungrouped*.
   f. Select **Normal** from the **Action** list.
   g. Click **OK**.

*Figure 60 Adding an IP address group*

3. Add a portal device:
   a. Select **Access Service > Portal Service Management > Device** from the navigation tree to enter the portal device configuration page.
   b. Click **Add** to enter the page shown in **Figure 61**.
   c. Enter the device name **NAS**.
   d. Enter the IP address of the switch’s interface connected to the host.
   e. Enter the key, which must be the same as that configured on the switch.
   f. Set whether to enable IP address reallocation.
      This example uses direct portal authentication, and therefore select **No** from the **Reallocate IP list**.
g. Set whether to support the portal server heartbeat and user heartbeat functions. In this example, select **Yes** for both **Support Server Heartbeat** and **Support User Heartbeat**.

h. Click OK.

**Figure 61 Adding a portal device**

![Add Device](image)

4. Associate the portal device with the IP address group:
   a. As shown in **Figure 62**, click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.

**Figure 62 Device list**

![Device List](image)

b. Click **Add** to enter the page shown in **Figure 63**.

**Figure 63 Port group configuration**

![Port Group Configuration](image)

c. Enter the port group name.

d. Select the configured IP address group.

172
The IP address used by the user to access the network must be within this IP address group.

e. User default values for other parameters.

f. Click OK.

5. Select Access Service > Service Parameters > Validate System Configuration from the navigation tree to validate the configurations.

Configuring the portal authentication server on IMC PLAT 5.0

This example assumes that the portal server runs on IMC PLAT 5.0(E0101) and IMC UAM 5.0(E0101).

1. Configure the portal authentication server:

   a. Log in to IMC and click the Service tab.

   b. Select User Access Manager > Portal Service Management > Server from the navigation tree to enter the portal server configuration page, as shown in Figure 64.

   c. Configure the portal server heartbeat interval and user heartbeat interval.

   d. Use the default settings for other parameters.

   e. Click OK.

Figure 64 Portal authentication server configuration

2. Configure the IP address group:

   a. Select User Access Manager > Portal Service Management > IP Group from the navigation tree to enter the portal IP address group configuration page.

   b. Click Add to enter the page shown in Figure 65.

   c. Enter the IP group name.

   d. Enter the start IP address and end IP address of the IP group.

   Make sure the host IP address is in the IP group.

   e. Select a service group.

   This example uses the default group Ungrouped.

   f. Select Normal from the Action list.
g. Click OK.

Figure 65 Adding an IP address group

<table>
<thead>
<tr>
<th>Add IP Group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Group Name</strong></td>
</tr>
<tr>
<td><strong>Start IP</strong></td>
</tr>
<tr>
<td><strong>End IP</strong></td>
</tr>
<tr>
<td><strong>Service Group</strong></td>
</tr>
<tr>
<td><strong>Action</strong></td>
</tr>
</tbody>
</table>

3. Add a portal device:
   a. Select User Access Manager > Portal Service Management > Device from the navigation tree to enter the portal device configuration page.
   b. Click Add to enter the page shown in Figure 66.
   c. Enter the device name NAS.
   d. Enter the IP address of the switch's interface connected to the host.
   e. Enter the key, which must be the same as that configured on the switch.
   f. Set whether to enable IP address reallocation.
      This example uses direct portal authentication, and therefore select No from the Reallocate IP list.
   g. Select whether to support sever heartbeat and user heartbeat functions.
      In this example, select Yes for both Support Server Heartbeat and Support User Heartbeat.
   h. Click OK.

Figure 66 Adding a portal device

<table>
<thead>
<tr>
<th>Add Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Name</strong></td>
</tr>
<tr>
<td><strong>Version</strong></td>
</tr>
<tr>
<td><strong>Listening Port</strong></td>
</tr>
<tr>
<td><strong>Authentication Retries</strong></td>
</tr>
<tr>
<td><strong>Reallocate IP</strong></td>
</tr>
<tr>
<td><strong>Support Server Heartbeat</strong></td>
</tr>
<tr>
<td><strong>Service Group</strong></td>
</tr>
<tr>
<td><strong>Device Description</strong></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
</tr>
<tr>
<td><strong>Key</strong></td>
</tr>
<tr>
<td><strong>Local Challenge</strong></td>
</tr>
<tr>
<td><strong>Logout Retries</strong></td>
</tr>
<tr>
<td><strong>Support User Heartbeat</strong></td>
</tr>
</tbody>
</table>

4. Associate the portal device with the IP address group:
a. As shown in Figure 67, click the icon in the Port Group Information Management column of device NAS to enter the port group configuration page.

b. Click Add to enter the page shown in Figure 68.

c. Enter the port group name.

d. Select the configured IP address group.
   The IP address used by the user to access the network must be within this IP address group.

e. Use the default settings for other parameters.

f. Click OK.

**Figure 67 Device list**

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Version</th>
<th>Service Group</th>
<th>IP Address</th>
<th>Port Group Information Management</th>
<th>Details</th>
<th>Modify</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS</td>
<td>Portal 2.0</td>
<td>Ungrouped</td>
<td>2.22.23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 68 Adding a port group**

5. Select User Access Manager > Service Parameters > Validate System Configuration from the navigation tree to validate the configurations.

**Configuring the switch**

1. Configure a RADIUS scheme:
   
   # Create a RADIUS scheme named rs1 and enter its view.
   
   `<Switch> system-view
   [Switch] radius scheme rs1
   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
   [Switch-radius-rs1] primary authentication 192.168.0.112
   [Switch-radius-rs1] primary accounting 192.168.0.112
   [Switch-radius-rs1] key authentication simple radius
   [Switch-radius-rs1] key accounting simple radius
   # Exclude the ISP domain name from the username sent to the RADIUS server.```
[Switch-radius-rsl] user-name-format without-domain
[Switch-radius-rsl] quit

# Enable RADIUS session control.
[Switch] radius session-control enable

2. Configure an authentication domain:

# Create an ISP domain named dm1 and enter its view.
[Switch] domain dm1

# Configure AAA methods for the ISP domain.
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit

# Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
[Switch] domain default enable dm1

3. Configure portal authentication:

# Configure a portal authentication server.
[Switch] portal server newpt
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100

# Configure reachability detection of the portal authentication server: set the server detection interval to 40 seconds, and send log messages upon reachability status changes.
[Switch-portal-server-newpt] server-detect timeout 40 log

NOTE:
The value of **timeout** must be greater than or equal to the portal server heartbeat interval.

# Configure portal user synchronization with the portal authentication server, and set the synchronization detection interval to 600 seconds.
[Switch-portal-server-newpt] user-sync timeout 600
[Switch-portal-server-newpt] quit

NOTE:
The value of **timeout** must be greater than or equal to the portal user heartbeat interval.

# Configure a portal Web server.
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] quit

# Enable direct portal authentication on VLAN-interface 100.
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method direct

# Enable portal fail-permit for the portal authentication server newpt.
[Switch-Vlan-interface100] portal fail-permit server newpt

# Reference the portal Web server newpt on VLAN-interface 100.
[Switch-Vlan-interface100] portal apply web-server newpt

# Configure the BAS-IP as 2.2.2.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.
Verifying the configuration

# Use the following command to display information about the portal authentication server.

[Switch] display portal server newpt

Portal server: newpt
  IP                    : 192.168.0.111
  VPN instance          : Not configured
  Port                  : 50100
  Server Detection      : Timeout 40s  Action: log
  User synchronization  : Timeout 600s
  Status                : Up

The Up status of the portal authentication server indicates that the portal authentication server is reachable. If the access device detects that the portal authentication server is unreachable, the Status field in the command output displays Down. The access device generates a server unreachable log "Portal server newpt turns down from up" and disables portal authentication on the access interface, so the host can access the external network without authentication.

Configuring cross-subnet portal authentication for MPLS L3VPNs

Network requirements

As shown in Figure 69, the PE device Switch A provides portal authentication for the host in VPN 1. A portal server in VPN 3 acts as the portal authentication server, portal Web server, and RADIUS server.

Configure cross-subnet portal authentication on Switch A, so the host can access Internet resources after passing identity authentication.

Figure 69 Network diagram

Configuration prerequisites

- Before enabling portal authentication, configure MPLS L3VPN and specify VPN targets for VPN 1 and VPN 3 so that VPN 1 and VPN 3 can communicate with each other. This example describes only the access authentication configuration on the user-side PE. For information about MPLS L3VPN configurations, see MPLS Configuration Guide.
- Configure the RADIUS server properly to provide authentication and accounting functions.

Configuration procedure

Perform the following tasks on Switch A.

1. Configure a RADIUS scheme:
   
   # Create a RADIUS scheme named rs1 and enter its view.
<SwitchA> system-view

[SwitchA] radius scheme rs1

# For the RADIUS scheme, specify the VPN instance that is bound to the interface connected to the portal/RADIUS server. This example uses VPN instance vpn3.
[SwitchA-radius-rs1] vpn-instance vpn3

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
[SwitchA-radius-rs1] primary authentication 192.168.0.111
[SwitchA-radius-rs1] primary accounting 192.168.0.111
[SwitchA-radius-rs1] key accounting simple radius
[SwitchA-radius-rs1] key authentication simple radius

# Exclude the ISP domain name from the username sent to the RADIUS server.
[SwitchA-radius-rs1] user-name-format without-domain

# Specify the source IP address for RADIUS packets to be sent as 3.3.0.3. This address must be the same as that of the portal device specified on the portal authentication server to avoid authentication failures.
[SwitchA-radius-rs1] nas-ip 3.3.0.3
[SwitchA-radius-rs1] quit

# Enable RADIUS session control.
[SwitchA] radius session-control enable

2. Configure an authentication domain:

# Create an ISP domain named dm1 and enter its view.
[SwitchA] domain dm1

# Configure AAA methods for the ISP domain.
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
[SwitchA-isp-dm1] quit

# Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
[SwitchA] domain default enable dm1

3. Configure portal authentication:

# Configure a portal authentication server.
[SwitchA] portal server newpt
[SwitchA-portal-server-newpt] ip 192.168.0.111 vpn-instance vpn3 key simple portal
[SwitchA-portal-server-newpt] port 50100
[SwitchA-portal-server-newpt] quit

# Configure a portal Web server.
[SwitchA] portal web-server newpt
[SwitchA-portal-websvr-newpt] vpn-instance vpn3
[SwitchA-portal-websvr-newpt] quit

# Enable cross-subnet portal authentication on VLAN-interface 3.
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] portal enable method layer3

# Reference the portal Web server newpt on VLAN-interface 3.
[SwitchA-Vlan-interface3] portal apply web-server newpt
# Configure the BAS-IP as 3.3.0.3 for portal packets sent from VLAN-interface 3 to the portal authentication server.

```bash
[SwitchA-Vlan-interface3] portal bas-ip 3.3.0.3
[SwitchA-Vlan-interface3] quit
```

Verifying the configuration

# Verify the portal configuration by executing the `display portal interface` command. (Details not shown.)

# After the user passes authentication, execute the `display portal user` command to display the portal user information.

```
[SwitchA] display portal user all
Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: None
  VPN instance: vpn3
  MAC                IP                 VLAN   Interface
  000d-88f7-c268     3.3.0.1            3      Vlan-interface3
```

Configuring direct portal authentication using local portal Web server

Network requirements

As shown in Figure 70, the host is directly connected to the switch (the access device). The host is assigned a public IP address either manually or through DHCP. The switch acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication on the switch. Before a user passes portal authentication, the user can access only the local portal Web server. After passing portal authentication, the user can access other network resources.

Figure 70 Network diagram

Configuration prerequisites and guidelines

- Configure IP addresses for the host, switch, and server as shown in Figure 70 and make sure they can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.
- Customize the authentication pages, compress them to a file, and upload the file to the root directory of the storage medium of the switch.

Configuration procedure

1. Configure a RADIUS scheme:

```
# Create a RADIUS scheme named rs1 and enter its view.
```
<Switch> system-view

[Switch] radius scheme rs1

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.
[Switch-radius-rs1] primary authentication 192.168.0.112
[Switch-radius-rs1] primary accounting 192.168.0.112
[Switch-radius-rs1] key authentication simple radius
[Switch-radius-rs1] key accounting simple radius

# Configure the switch to remove the ISP domain name from the usernames sent to the RADIUS server.
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit

# Enable the RADIUS session-control feature.
[Switch] radius session-control enable

2. Configure an authentication domain:

# Create an ISP domain named dm1 and enter its view.
[Switch] domain dm1

# Configure AAA methods for the ISP domain.
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit

# Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.
[Switch] domain default enable dm1

3. Configure portal authentication:

# Configure the portal Web server name as newpt and URL as the IP address of the portal authentication-enabled interface or a loopback interface (except 127.0.0.1).
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://2.2.2.1:2331/portal
[Switch-portal-websvr-newpt] quit

# Enable direct portal authentication on VLAN-interface 100.
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method direct

# Specify the portal Web server newpt on VLAN-interface 100.
[Switch-Vlan-interface100] portal apply web-server newpt
[Switch-Vlan-interface100] quit

# Create a local portal Web server. Use HTTP to exchange authentication information with clients.
[Switch] portal local-web-server http

# Specify file abc.zip as the default authentication page file for local portal authentication. (Make sure the file exist under the root directory of the switch.)
[Switch-portal-local-websvr-http] default-logon-page abc.zip

# Set the HTTP service listening port number to 2331 for the local portal Web server.
[Switch-portal-local-websvr-http] tcp-port 2331
[Switch-portal-local-websvr-http] quit
Verifying the configuration

# Verify that the portal configuration has taken effect.

[Switch] display portal interface vlan-interface 100

Portal information of Vlan-interface 100

VSRP instance: --
VSRP state: N/A
Authorization                   Strict checking
ACL                             Disabled
User profile                    Disabled

IPv4:
Portal status: Enabled
Authentication type: Direct
Portal Web server: newpt
Authentication domain: Not configured
Pre-auth IP pool: Not configured
BAS-IP: Not configured
User Detection: Not configured
Action for server detection:

<table>
<thead>
<tr>
<th>Server type</th>
<th>Server name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

Layer3 source network:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Mask</th>
</tr>
</thead>
</table>

Destination authenticate subnet:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Mask</th>
</tr>
</thead>
</table>

IPv6:
Portal status: Disabled
Authentication type: Disabled
Portal Web server: Not configured
Authentication domain: Not configured
Pre-auth IP pool: Not configured
BAS-IPv6: Not configured
User detection: Not configured
Action for server detection:

<table>
<thead>
<tr>
<th>Server type</th>
<th>Server name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
</tbody>
</table>

Layer3 source network:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Prefix length</th>
</tr>
</thead>
</table>

Destination authenticate subnet:

<table>
<thead>
<tr>
<th>IP address</th>
<th>Prefix length</th>
</tr>
</thead>
</table>

A user can perform portal authentication through a Web page. Before passing the authentication, the user can access only the authentication page http://2.2.2.1:2331/portal and all Web requests will be redirected to the authentication page. After passing the authentication, the user can access other network resources.

# After the user passes authentication, use the following command to display information about the portal user.

[Switch] display portal user interface vlan-interface 100
Total portal users: 1
Username: abc
Portal server: newpt
State: Online
VPN instance: --

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0015-e9a6-7cfe</td>
<td>2.2.2.2</td>
<td>--</td>
<td>vlan-interface 100</td>
</tr>
</tbody>
</table>

Authorization information:
- IP pool: N/A
- User profile: N/A
- Session group profile: N/A
- ACL: N/A
- CAR: N/A

Troubleshooting portal

No portal authentication page is pushed for users

Symptom
When a user is redirected to the IMC portal authentication server, no portal authentication page or error message is prompted for the user. The login page is blank.

Analysis
The key configured on the portal access device and that configured on the portal authentication server are inconsistent. As a result, packet verification fails, and the portal authentication server refuses to push the authentication page.

Solution
Use the `display portal server` command on the access device to check whether a key is configured for the portal authentication server.
- If no key is configured, configure the right key.
- If a key is configured, use the `ip` or `ipv6` command in the portal authentication server view to correct the key, or correct the key configured for the access device on the portal authentication server.

Cannot log out portal users on the access device

Symptom
You cannot use the `portal delete-user` command on the access device to log out a portal user, but the portal user can log out by clicking the Disconnect button on the portal authentication client.

Analysis
When you execute the `portal delete-user` command on the access device to log out a user, the access device sends an unsolicited logout notification message to the portal authentication server. The destination port number in the logout notification is the listening port number of the portal authentication server configured on the access device. If this listening port number is not the actual listening port number configured on the server, the server cannot receive the notification. As a result, the portal server does not log out the user.

When a user uses the Disconnect button on the authentication client to log out, the portal authentication server sends an unsolicited logout request message to the access device. The
access device uses the source port in the logout request as the destination port in the logout ACK message. As a result, the portal authentication server can definitely receive the logout ACK message and log out the user.

Solution
1. Use the `display portal server` command to display the listening port of the portal authentication server configured on the access device.
2. Use the `portal server` command in system view to change the listening port number to the actual listening port of the portal authentication server.

Cannot log out portal users on the RADIUS server

Symptom
The access device uses the HPE IMC server as the RADIUS server to perform identity authentication for portal users. You cannot log out the portal users on the RADIUS server.

Analysis
The HPE IMC server uses session control packets to send disconnection requests to the access device. On the access device, the listening UDP port for session control packets is disabled by default. Therefore, the access device cannot receive the portal user logout requests from the RADIUS server.

Solution
On the access device, execute the `radius session-control enable` command in system view to enable the RADIUS session control function.

Users logged out by the access device still exist on the portal authentication server

Symptom
After you log out a portal user on the access device, the user still exists on the portal authentication server.

Analysis
When you execute the `portal delete-user` command on the access device to log out a user, the access device sends an unsolicited logout notification to the portal authentication server. If the BAS-IP or BAS-IPv6 address carried in the logout notification is different from the portal device IP address specified on the portal authentication server, the portal authentication server discards the logout notification. When sending of the logout notifications times out, the access device logs out the user. However, the portal authentication server does not receive the logout notification successfully, and therefore it regards the user is still online.

Solution
Configure the BAS-IP or BAS-IPv6 attribute on the interface enabled with portal authentication. Make sure the attribute value is the same as the portal device IP address specified on the portal authentication server.
Re-DHCP portal authenticated users cannot log in successfully

Symptom
The device performs re-DHCP portal authentication for users. A user enters the correct username and password, and the client successfully obtains the private and public IP addresses. However, the authentication result for the user is failure.

Analysis
When the access device detects that the client IP address is changed, it sends an unsolicited portal packet to notify of the IP change to the portal authentication server. The portal authentication server notifies of the authentication success only after it receives the IP change notification from both the access device and the client.

If the BAS-IP or BAS-IPv6 address carried in the portal notification packet is different from the portal device IP address specified on the portal authentication server, the portal authentication server discards the portal notification packet. As a result, the portal authentication server considers that the user has failed the authentication.

Solution
Configure the BAS-IP or BAS-IPv6 attribute on the interface enabled with portal authentication. Make sure the attribute value is the same as the portal device IP address specified on the portal authentication server.
Configuring port security

Overview

Port security combines and extends 802.1X and MAC authentication to provide MAC-based network access control. This feature applies to networks, such as a WLAN, that require different authentication methods for different users on a port.

Port security provides the following functions:

- Prevents unauthorized access to a network by checking the source MAC address of inbound traffic.
- Prevents access to unauthorized devices or hosts by checking the destination MAC address of outbound traffic.
- Controls MAC address learning and authentication on a port to make sure the port learns only source trusted MAC addresses.

A frame is illegal if its source MAC address cannot be learned in a port security mode or it is from a client that has failed 802.1X or MAC authentication. The port security feature automatically takes a predefined action on illegal frames. This automatic mechanism enhances network security and reduces human intervention.

NOTE:
As a best practice, use the 802.1X authentication or MAC authentication feature rather than port security for scenarios that require only 802.1X authentication or MAC authentication. For more information about 802.1X and MAC authentication, see "Configuring 802.1X" and "Configuring MAC authentication."

Port security features

NTK

The need to know (NTK) feature prevents traffic interception by checking the destination MAC address in the outbound frames. The feature ensures that frames are sent only to the following hosts:

- Hosts that have passed authentication.
- Hosts whose MAC addresses have been learned or configured on the access device.

Intrusion protection

The intrusion protection feature checks the source MAC address in inbound frames for illegal frames, and takes a predefined action on each detected illegal frame. The action can be disabling the port temporarily, disabling the port permanently, or blocking frames from the illegal MAC address for 3 minutes (not user configurable).

Port security modes

Port security supports the following categories of security modes:

- **MAC learning control**—Includes two modes: autoLearn and secure. MAC address learning is permitted on a port in autoLearn mode and disabled in secure mode.
- **Authentication**—Security modes in this category implement MAC authentication, 802.1X authentication, or a combination of these two authentication methods.
Upon receiving a frame, the port in a security mode searches the MAC address table for the source MAC address. If a match is found, the port forwards the frame. If no match is found, the port learns the MAC address or performs authentication, depending on the security mode. If the frame is illegal, the port takes the predefined NTK or intrusion protection action. Outgoing frames are not restricted by port security's NTK action unless they trigger the NTK feature.

The maximum number of users a port supports equals the smaller value from the following values:
- The maximum number of secure MAC addresses that port security allows.
- The maximum number of concurrent users the authentication mode in use allows.

For example, if 802.1X allows more concurrent users than port security's limit on the number of MAC addresses on the port in userLoginSecureExt mode, port security's limit takes effect.

Table 15 describes the port security modes and the security features.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Security mode</th>
<th>Features that can be triggered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turning off the port security feature</td>
<td>noRestrictions (the default mode) In this mode, port security is disabled on the port and access to the port is not restricted.</td>
<td>N/A</td>
</tr>
<tr>
<td>Controlling MAC address learning</td>
<td>autoLearn secure</td>
<td>NTK/intrusion protection</td>
</tr>
<tr>
<td>Performing 802.1X authentication</td>
<td>userLogin userLoginSecure userLoginSecureExt userLoginWithOUI</td>
<td>N/A</td>
</tr>
<tr>
<td>Performing MAC authentication</td>
<td>macAddressWithRadius</td>
<td>NTK/intrusion protection</td>
</tr>
<tr>
<td>Performing a combination of MAC authentication and 802.1X authentication</td>
<td>Or</td>
<td>macAddressOrUserLoginSecure macAddressOrUserLoginSecureExt macAddressElseUserLoginSecure macAddressElseUserLoginSecureExt</td>
</tr>
</tbody>
</table>

**TIP:**
- **userLogin** specifies 802.1X authentication and port-based access control. **userLogin** with **Secure** specifies 802.1X authentication and MAC-based access control. **Ext** indicates allowing multiple 802.1X users to be authenticated and serviced at the same time. A security mode without **Ext** allows only one user to pass 802.1X authentication.
- **macAddress** specifies MAC authentication.
- **Else** specifies that the authentication method before **Else** is applied first. If the authentication fails, whether to turn to the authentication method following **Else** depends on the protocol type of the authentication request.
- In a security mode with **Or**, the authentication method to be used depends on the protocol type of the authentication request.

**Controlling MAC address learning**
- **autoLearn.**
A port in this mode can learn MAC addresses. The automatically learned MAC addresses are not added to the MAC address table as dynamic MAC address. Instead, these MAC addresses are added to the secure MAC address table as secure MAC addresses. You can also configure secure MAC addresses by using the `port-security mac-address security` command.

A port in autoLearn mode allows frames sourced from the following MAC addresses to pass:
- Secure MAC addresses.
- MAC addresses configured by using the `mac-address dynamic` and `mac-address static` commands.

When the number of secure MAC addresses reaches the upper limit, the port transitions to secure mode.

- secure.

MAC address learning is disabled on a port in secure mode. You configure MAC addresses by using the `mac-address static` and `mac-address dynamic` commands. For more information about configuring MAC address table entries, see Layer 2—LAN Switching Configuration Guide.

A port in secure mode allows only frames sourced from the following MAC addresses to pass:
- Secure MAC addresses.
- MAC addresses configured by using the `mac-address dynamic` and `mac-address static` commands.

Performing 802.1X authentication

- userLogin.
  A port in this mode performs 802.1X authentication and implements port-based access control. The port can service multiple 802.1X users. Once an 802.1X user passes authentication on the port, any subsequent 802.1X users can access the network through the port without authentication.

- userLoginSecure.
  A port in this mode performs 802.1X authentication and implements MAC-based access control. The port services only one user passing 802.1X authentication.

- userLoginSecureExt.
  This mode is similar to the userLoginSecure mode except that this mode supports multiple online 802.1X users.

- userLoginWithOUI.
  This mode is similar to the userLoginSecure mode. The difference is that a port in this mode also permits frames from one user whose MAC address contains a specific OUI.

  In this mode, the port performs OUI check first. If the OUI check fails, the port performs 802.1X authentication. The port permits frames that pass OUI check or 802.1X authentication.

**NOTE:**

An OUI is a 24-bit number that uniquely identifies a vendor, manufacturer, or organization. In MAC addresses, the first three octets are the OUI.

Performing MAC authentication

macAddressWithRadius: A port in this mode performs MAC authentication, and services multiple users.

Performing a combination of MAC authentication and 802.1X authentication

- macAddressOrUserLoginSecure.
  This mode is the combination of the macAddressWithRadius and userLoginSecure modes. The mode allows one 802.1X authentication user and multiple MAC authentication users to log in.
In this mode, the port performs 802.1X authentication first. If 802.1X authentication fails, MAC authentication is performed.

- **macAddressOrUserLoginSecureExt.**
  This mode is similar to the macAddressOrUserLoginSecure mode, except that this mode supports multiple 802.1X and MAC authentication users.

- **macAddressElseUserLoginSecure.**
  This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority as the Else keyword implies. The mode allows one 802.1X authentication user and multiple MAC authentication users to log in.
  The port performs MAC authentication upon receiving non-802.1X frames. Upon receiving 802.1X frames, the port performs MAC authentication and then, if the authentication fails, 802.1X authentication.

- **macAddressElseUserLoginSecureExt.**
  This mode is similar to the macAddressElseUserLoginSecure mode except that this mode supports multiple 802.1X and MAC authentication users as the Ext keyword implies.

### Configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling port security</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Setting port security's limit on the number of secure MAC addresses on a port</td>
<td>N/A</td>
</tr>
<tr>
<td>(Required.) Setting the port security mode</td>
<td>N/A</td>
</tr>
<tr>
<td>(Required.) Configuring port security features:</td>
<td>N/A</td>
</tr>
<tr>
<td>• Configuring NTK</td>
<td>Configure one or more port security features according to the network requirements.</td>
</tr>
<tr>
<td>• Configuring intrusion protection</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring secure MAC addresses</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Ignoring authorization information from the server</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Enabling MAC move</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Applying a NAS-ID profile to port security</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Enabling the authorization-fail-offline feature</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Enabling SNMP notifications for port security</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Enabling port security

Before you enable port security, disable 802.1X and MAC authentication globally.

When port security is enabled, you cannot enable 802.1X or MAC authentication, or change the access control mode or port authorization state. Port security automatically modifies these settings in different security modes.

To enable port security:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable port security.</td>
<td>port-security enable</td>
<td>By default, port security is</td>
</tr>
</tbody>
</table>
You can use the `undo port-security enable` command to disable port security. Because the command logs off the online users, make sure no online users are present.

Enabling or disabling port security resets the following security settings to the default:
- 802.1X access control mode is MAC based.
- 802.1X port authorization state is auto.

For more information about 802.1X authentication and MAC authentication configuration, see "Configuring 802.1X" and "Configuring MAC authentication."

### Setting port security's limit on the number of secure MAC addresses on a port

You can set the maximum number of secure MAC addresses that port security allows on a port for the following purposes:
- Controlling the number of concurrent users on the port.
  - For a port operating in a security mode (except for autoLearn and secure), the upper limit equals the smaller of the following values:
    - The limit of the secure MAC addresses that port security allows.
    - The limit of concurrent users allowed by the authentication mode in use.
- Controlling the number of secure MAC addresses on the port in autoLearn mode.

The port security's limit on the number of secure MAC addresses on a port is independent of the MAC learning limit described in MAC address table configuration. For more information about MAC address table configuration, see Layer 2—LAN Switching Configuration Guide.

You can set the maximum number of secure MAC addresses that port security allows for specific VLANs on a port when the port security mode is autoLearn. When the maximum number is exceeded, intrusion protection will be triggered in the specified VLANs.

To set the maximum number of secure MAC addresses allowed on a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Set the maximum number of secure MAC addresses allowed on a port.</td>
<td>port-security max-mac-count count-value [ vlan [ vlan-id-list ] ]</td>
</tr>
</tbody>
</table>

### Setting the port security mode

Before you set a port security mode for a port, complete the following tasks:
- Disable 802.1X and MAC authentication.
- Verify that the port does not belong to any aggregation group or service loopback group.
If you are configuring the autoLearn mode, set port security’s limit on the number of secure MAC addresses. You cannot change the setting when the port is operating in autoLearn mode.

When you set the port security mode, follow these guidelines:

- You can specify a port security mode when port security is disabled, but your configuration cannot take effect.
- Changing the port security mode of a port logs off the online users of the port.
- Do not enable 802.1X authentication or MAC authentication on a port where port security is configured.

To enable a port security mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Set an OUI value for user authentication.</td>
<td>port-security oui index-value mac-address</td>
</tr>
<tr>
<td>3.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Set the port security mode.</td>
<td>port-security port-mode { autolearn</td>
</tr>
</tbody>
</table>

Configuring port security features

Configuring NTK

The NTK feature checks the destination MAC addresses in outbound frames to make sure frames are forwarded only to authenticated devices.

The NTK feature supports the following modes:

- **ntkonly**—Forwards only unicast frames with authenticated destination MAC addresses.
- **ntk-withbroadcasts**—Forwards only broadcast frames and unicast frames with authenticated destination MAC addresses.
- **ntk-withmulticasts**—Forwards only broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses.
The NTK feature drops any unicast frame with an unknown destination MAC address. Not all port security modes support triggering the NTK feature. For more information, see Table 15.

To configure the NTK feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the NTK feature.</td>
<td>port-security ntk-mode { ntk-withbroadcasts</td>
</tr>
</tbody>
</table>

**Configuring intrusion protection**

Intrusion protection enables a device to take one of the following actions in response to illegal frames:

- **blockmac**—Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards the frames. All subsequent frames sourced from a blocked MAC address are dropped. A blocked MAC address is restored to normal state after being blocked for 3 minutes. The interval is fixed and cannot be changed.
- **disableport**—Disables the port until you bring it up manually.
- **disableport-temporarily**—Disables the port for a period of time. The period can be configured with the `port-security timer disableport` command.

To configure the intrusion protection feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the intrusion protection feature.</td>
<td>port-security intrusion-mode { blockmac</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Set the silence timeout period during which a port remains disabled.</td>
<td>port-security timer disableport time-value</td>
</tr>
</tbody>
</table>

**NOTE:**

On a port operating in either macAddressElseUserLoginSecure mode or macAddressElseUserLoginSecureExt mode, intrusion protection is triggered only after both MAC authentication and 802.1X authentication fail for the same frame.

**Configuring secure MAC addresses**

Secure MAC addresses are configured or learned in autoLearn mode. If the secure MAC addresses are saved, they can survive a device reboot. You can bind a secure MAC address only to one port in a VLAN.
When the maximum number of secure MAC address entries is reached, the port changes to secure mode. In secure mode, the port cannot add or learn any more secure MAC addresses. The port allows only frames sourced from secure MAC addresses or MAC addresses configured by using the `mac-address dynamic` or `mac-address static` command to pass through.

### Table 16 A comparison of static, sticky, and dynamic secure MAC addresses

<table>
<thead>
<tr>
<th>Type</th>
<th>Address sources</th>
<th>Aging mechanism</th>
<th>Can be saved and survive a device reboot?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>Manually added (by using the <code>port-security mac-address security</code> command without the <code>sticky</code> keyword).</td>
<td>Not available. The static addresses never age out unless you perform any of the following tasks: • Manually remove these MAC addresses. • Change the port security mode. • Disable the port security feature.</td>
<td>Yes.</td>
</tr>
<tr>
<td>Sticky</td>
<td>• Manually added (by using the <code>port-security mac-address security</code> command with the <code>sticky</code> keyword). • Converted from dynamic secure MAC addresses. • Automatically learned when the dynamic secure MAC feature (<code>port-security mac-address dynamic</code>) is disabled.</td>
<td>By default, sticky MAC addresses do not age out. However, you can configure an aging timer or use the aging timer together with the inactivity aging feature to delete old sticky MAC addresses. • If only the aging timer is configured, the aging timer counts up regardless of whether traffic data has been sent from the sticky MAC address. • If both the aging timer and the inactivity aging feature are configured, the aging timer restarts once traffic data is detected from the sticky MAC address.</td>
<td>Yes. The secure MAC aging timer restarts at a reboot.</td>
</tr>
<tr>
<td>Dynamic</td>
<td>• Converted from sticky MAC addresses. • Automatically learned after the dynamic secure MAC feature is enabled.</td>
<td>Same as sticky MAC addresses.</td>
<td>No. All dynamic secure MAC addresses are lost at reboot.</td>
</tr>
</tbody>
</table>

### Configuration prerequisites

Before you configure secure MAC addresses, complete the following tasks:

- Enable port security.
- Set port security's limit on the number of MAC addresses on the port. Perform this task before you enable autoLearn mode.
- Set the port security mode to autoLearn.
- Configure the port to permit packets of the specified VLAN to pass or add the port to the VLAN. Make sure the VLAN already exists.

### Configuration procedure

To configure a secure MAC address:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. (Optional.) Set the secure MAC aging timer.</td>
<td>port-security timer autolearn aging time-value</td>
<td>By default, secure MAC addresses do not age out.</td>
</tr>
</tbody>
</table>
| 3. Configure a secure MAC address. | \- In system view: port-security mac-address security [ sticky ] mac-address interface interface-type interface-number vlan vlan-id  
\- In Layer 2 Ethernet interface view:  
a. interface interface-type interface-number  
b. port-security mac-address security [ sticky ] mac-address vlan vlan-id  
c. quit | By default, no secure MAC address exists.  
In the same VLAN, a MAC address cannot be specified as both a static secure MAC address and a sticky MAC address. |
| 4. Enter Layer 2 Ethernet interface view. | interface interface-type interface-number | N/A |
| 5. (Optional.) Enable inactivity aging. | port-security mac-address aging-type inactivity | By default, the inactivity aging feature is disabled. |
| 6. (Optional.) Enable the dynamic secure MAC feature. | port-security mac-address dynamic | By default, the dynamic secure MAC feature is disabled. Sticky MAC addresses can be saved to the configuration file. Once saved, they can survive a device reboot. |

## Ignoring authorization information from the server

You can configure a port to ignore the authorization information received from the server (local or remote) after an 802.1X or MAC authentication user passes authentication.

To configure a port to ignore authorization information from the server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter Layer 2 Ethernet interface view.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Ignore the authorization information received from the authentication server.</td>
<td>port-security authorization ignore</td>
<td>By default, a port uses the authorization information received from the authentication server.</td>
</tr>
</tbody>
</table>

## Enabling MAC move

MAC move allows 802.1X or MAC authenticated users to move between ports on a device. For example, if an authenticated 802.1X user moves to another 802.1X-enabled port on the device, the authentication session is deleted from the first port. The user is reauthenticated on the new port.

If MAC move is disabled and an 802.1X authenticated user moves to another port, the user is not reauthenticated.
As a best practice, enable MAC move for wireless users that roam between ports to access the network.

To enable MAC move:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable MAC move.</td>
<td>port-security mac-move permit</td>
</tr>
</tbody>
</table>

Applying a NAS-ID profile to port security

By default, the device sends its device name in the NAS-Identifier attribute of all RADIUS requests.

A NAS-ID profile enables you to send different NAS-Identifier attribute strings in RADIUS requests from different VLANs. The strings can be organization names, service names, or any user categorization criteria, depending on the administrative requirements.

For example, map the NAS-ID **companyA** to all VLANs of company A. The device will send **companyA** in the NAS-Identifier attribute for the RADIUS server to identify requests from any Company A users.

You can apply a NAS-ID profile to port security globally or on a port. On a port, the device selects a NAS-ID profile in the following order:

1. The port-specific NAS-ID profile.
2. The NAS-ID profile applied globally.

If no NAS-ID profile is applied or no matching binding is found in the selected profile, the device uses the device name as the NAS-ID.

For more information about the NAS-ID profile configuration, see "Configuring AAA."

To apply a NAS-ID profile to port security:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Apply a NAS-ID profile to port security. | - In system view: port-security nas-id-profile profile-name  
- In Layer 2 Ethernet interface view:  
  a. interface interface-type interface-number  
  b. port-security nas-id-profile profile-name | By default, no NAS-ID profile is applied in system view or in Layer 2 Ethernet interface view. |

Enabling the authorization-fail-offline feature

The authorization-fail-offline feature logs off port security users who fail ACL or user profile authorization.

A user fails ACL or user profile authorization in the following situations:

- The device fails to authorize the specified ACL or user profile to the user.
- The server assigns a nonexistent ACL or user profile to the user.
This feature does not apply to VLAN authorization failure. The device logs off these users directly.

To enable the authorization-fail-offline feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable the authorization-fail-offline feature.</td>
<td>port-security authorization-fail offline</td>
<td>By default, this feature is disabled, and the device does not log off users who fail ACL or user profile authorization.</td>
</tr>
</tbody>
</table>

## Enabling SNMP notifications for port security

**IMPORTANT:**
This feature is available in Release 1121 and later.

Use this feature to report critical port security events to an NMS. For port security event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

For this feature to take effect, make sure the intrusion protection feature is configured.

To enable SNMP notifications for port security:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable SNMP notifications for port security.</td>
<td>snmp-agent trap enable port-security [ address-learned</td>
<td>dot1x-failure</td>
</tr>
</tbody>
</table>

## Displaying and maintaining port security

Execute `display` commands in any view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the port security configuration, operation information, and statistics.</td>
<td>display port-security [ interface interface-type interface-number ]</td>
</tr>
<tr>
<td>Display information about secure MAC addresses.</td>
<td>display port-security mac-address security [ interface interface-type interface-number ] [ vlan vlan-id ] [ count ]</td>
</tr>
<tr>
<td>Display information about blocked MAC addresses.</td>
<td>display port-security mac-address block [ interface interface-type interface-number ] [ vlan vlan-id ] [ count ]</td>
</tr>
</tbody>
</table>
Port security configuration examples

autoLearn configuration example

Network requirements

As shown in Figure 71, configure port GigabitEthernet 1/0/1 on the device to meet the following requirements:

- Accept up to 64 users without authentication.
- Be permitted to learn and add MAC addresses as sticky MAC addresses, and set the secure MAC aging timer to 30 minutes.
- Stop learning MAC addresses after the number of secure MAC addresses reaches 64. If any frame with an unknown MAC address arrives, intrusion protection starts, and the port shuts down and stays silent for 30 seconds.

Figure 71 Network diagram

![Network diagram]

Configuration procedure

# Enable port security.
<Device> system-view
[Device] port-security enable

# Set the secure MAC aging timer to 30 minutes.
[Device] port-security timer autolearn aging 30

# Set port security's limit on the number of secure MAC addresses to 64 on port GigabitEthernet 1/0/1.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64

# Set the port security mode to autoLearn.
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn

# Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.
[Device-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-GigabitEthernet1/0/1] quit
[Device] port-security timer disableport 30

Verifying the configuration

# Verify the port security configuration.
[Device] display port-security interface gigabitethernet 1/0/1

Port security parameters:

- Port security : Enabled
- AutoLearn aging time : 30 min
- Disableport timeout : 30 s
- MAC move : Denied
- Authorization fail : Online
NAS-ID profile is not configured
Dot1x-failure trap : Disabled
Dot1x-logon trap : Disabled
Dot1x-logoff trap : Enabled
Intrusion trap : Disabled
Address-learned trap : Enabled
Mac-auth-failure trap : Disabled
Mac-auth-logon trap : Enabled
Mac-auth-logoff trap : Disabled
OUI value list : 

GigabitEthernet1/0/1 is link-up
Port mode : autoLearn
NeedToKnow mode : Disabled
Intrusion protection mode : DisablePortTemporarily
Security MAC address attribute
  Learning mode : Sticky
  Aging type : Periodical
Max secure MAC addresses : 64
Current secure MAC addresses : 5
Authorization : Permitted
NAS-ID profile is not configured

The output shows the following information:
- The port security's limit on the number of secure MAC addresses on the port is 64.
- The port security mode is autoLearn.
- The intrusion protection action is disabling the port (DisablePortTemporarily) for 30 seconds.

The port allows for MAC address learning, and you can display the number of learned MAC addresses in the Current number of secure MAC addresses field.

# Display additional information about the learned MAC addresses.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] display this
# interface GigabitEthernet1/0/1
port-security max-mac-count 64
port-security port-mode autolearn
port-security mac-address security sticky 0002-0000-0015 vlan 1
port-security mac-address security sticky 0002-0000-0014 vlan 1
port-security mac-address security sticky 0002-0000-0013 vlan 1
port-security mac-address security sticky 0002-0000-0012 vlan 1
port-security mac-address security sticky 0002-0000-0011 vlan 1
#
[Device-GigabitEthernet1/0/1] quit

# Verify that the port security mode changes to secure after the number of MAC addresses learned by the port reaches 64.
[Device] display port-security interface gigabitethernet 1/0/1

# Verify that the port will be disabled for 30 seconds after it receives a frame with an unknown MAC address. (Details not shown.)
After the port is re-enabled, delete several secure MAC addresses.

[Device] undo port-security mac-address security sticky 0002-0000-0015 vlan 1
[Device] undo port-security mac-address security sticky 0002-0000-0014 vlan 1

Verify that the port security mode of the port changes to **autoLearn**, and the port can learn MAC addresses again. (Details not shown.)

### userLoginWithOUI configuration example

#### Network requirements

As shown in **Figure 72**, a client is connected to the device through port GigabitEthernet 1/0/1. The device authenticates the client with a RADIUS server. If the authentication succeeds, the client is authorized to access the Internet.

- The RADIUS server at 192.168.1.2 functions as the primary authentication server and the secondary accounting server. The RADIUS server at 192.168.1.3 functions as the secondary authentication server and the primary accounting server. The shared key for authentication is **name**, and the shared key for accounting is **money**.
- All users use the authentication, authorization, and accounting methods of ISP domain **sun**.
- The RADIUS server response timeout time is 5 seconds. The maximum number of RADIUS packet retransmission attempts is five. The device sends real-time accounting packets to the RADIUS server at 15-minute intervals, and sends usernames without domain names to the RADIUS server.

Configure port GigabitEthernet 1/0/1 of the device to allow only one 802.1X user and a user who uses one of the specified OUI values to be authenticated.

**Figure 72 Network diagram**

Configuration procedure

The following configuration steps cover some AAA/RADIUS configuration commands. For more information about the commands, see *Security Command Reference*.

Make sure the host and the RADIUS server can reach each other.

1. **Configure AAA:**

   # Configure a RADIUS scheme named **radsun**.

   ```
   <Device> system-view
   [Device] radius scheme radsun
   [Device-radius-radsun] primary authentication 192.168.1.2
   [Device-radius-radsun] primary accounting 192.168.1.3
   [Device-radius-radsun] secondary authentication 192.168.1.3
   [Device-radius-radsun] secondary accounting 192.168.1.2
   [Device-radius-radsun] key authentication simple name
   [Device-radius-radsun] key accounting simple money
   ```
[Device-radius-radsun] timer response-timeout 5
[Device-radius-radsun] retry 5
[Device-radius-radsun] timer realtime-accounting 15
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit

# Configure ISP domain sun.
[Device] domain sun
[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] quit

2. Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.
[Device] dot1x authentication-method chap

3. Configure port security:
   # Enable port security.
   [Device] port-security enable
   # Add five OUI values. (You can add up to 16 OUI values. The port permits only one user matching one of the OUIs to pass authentication.)
   [Device] port-security oui index 1 mac-address 1234-0100-1111
   [Device] port-security oui index 2 mac-address 1234-0200-1111
   [Device] port-security oui index 3 mac-address 1234-0300-1111
   [Device] port-security oui index 4 mac-address 1234-0400-1111
   [Device] port-security oui index 5 mac-address 1234-0500-1111
   # Set the port security mode to userLoginWithOUI.
   [Device] interface gigabitethernet 1/0/1
   [Device-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
   [Device-GigabitEthernet1/0/1] quit

Verifying the configuration

# Verify the RADIUS scheme configuration.
[Device] display radius scheme radsun
RADIUS Scheme Name : radsun
   Index : 0
   Primary Auth Server:
      IP : 192.168.1.2    Port: 1812    State: Active
      VPN : Not configured
   Primary Acct Server:
      IP : 192.168.1.3    Port: 1813    State: Active
      VPN : Not configured
   Second Auth Server:
      IP : 192.168.1.3    Port: 1812    State: Active
      VPN : Not configured
   Second Acct Server:
      IP : 192.168.1.2    Port: 1813    State: Active
      VPN : Not configured

   Accounting-On function : Disabled
   retransmission times : 50
retransmission interval (seconds) : 3
Timeout Interval (seconds) : 5
Retransmission Times : 5
Retransmission Times for Accounting Update : 5
Server Quiet Period (minutes) : 5
Realtime Accounting Interval (minutes) : 15
NAS IP Address : Not configured
VPN : Not configured
User Name Format : without-domain
Data flow unit : Byte
Packet unit : one
Attribute-15 check-mode : strict

# After users pass authentication, display port security configuration. Verify that port GigabitEthernet 1/0/1 allows only one 802.1X user to be authenticated.

[Device] display port-security interface gigabitethernet 1/0/1

Port security parameters:
Port security : Enabled
AutoLearn aging time : 0 min
Disableport timeout : 20 s
MAC move : Denied
Authorization fail : Online
NAS-ID profile is not configured
Dot1x-failure trap : Disabled
Dot1x-logon trap : Disabled
Dot1x-logoff trap : Enabled
Intrusion trap : Disabled
Address-learned trap : Enabled
Mac-auth-failure trap : Disabled
Mac-auth-logon trap : Enabled
Mac-auth-logoff trap : Disabled
OUI value list :
  Index : 1, Value : 123401
  Index : 2, Value : 123402
  Index : 3, Value : 123403
  Index : 4, Value : 123404
  Index : 5, Value : 123405

GigabitEthernet1/0/1 is link-up
Port mode : userLoginWithOUI
NeedToKnow mode : Disabled
Intrusion protection mode : NoAction
Security MAC address attribute
  Learning mode : Sticky
  Aging type : Periodical
Max secure MAC addresses : Not configured
Current secure MAC addresses : 1
Authorization : Permitted
NAS-ID profile is not configured
macAddressElseUserLoginSecure configuration example

Network requirements

As shown in Figure 73, a client is connected to the device through GigabitEthernet 1/0/1. The device authenticates the client by a RADIUS server. If the authentication succeeds, the client is authorized to access the Internet.

Configure port GigabitEthernet 1/0/1 of the device to meet the following requirements:

- Allow more than one MAC authenticated user to log on.
- For 802.1X users, perform MAC authentication first and then, if MAC authentication fails, 802.1X authentication. Allow only one 802.1X user to log on.
- Use the MAC address of each user as the username and password for authentication. A MAC address is in the hexadecimal notation with hyphens, and letters are in upper case.
- Set the total number of MAC authenticated users and 802.1X authenticated users to 64.
- Enable NTK (ntkonly mode) to prevent frames from being sent to unknown MAC addresses.

Figure 73 Network diagram

Configuration procedure

Make sure the host and the RADIUS server can reach each other.

1. Configure RADIUS authentication/accounting and ISP domain settings. (See "userLoginWithOUI configuration example.")

2. Configure port security:

   # Enable port security.
   <Device> system-view
   [Device] port-security enable
   # Use MAC-based accounts for MAC authentication. Each MAC address must be in the hexadecimal notation with hyphens, and letters are in upper case.
   [Device] mac-authentication user-name-format mac-address with-hyphen uppercase
   # Specify the MAC authentication domain.
   [Device] mac-authentication domain sun
# Set the 802.1X authentication method to CHAP. By default, the authentication method for 802.1X is CHAP.

[Device] dot1x authentication-method chap

# Set port security's limit on the number of MAC addresses to 64 on the port.

[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64

# Set the port security mode to macAddressElseUserLoginSecure.

[Device-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure

# Set the NTK mode of the port to ntkonly.

[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly

[Device-GigabitEthernet1/0/1] quit

Verifying the configuration

# Verify the port security configuration.

[Device] display port-security interface gigabitethernet 1/0/1

Port security parameters:
- Port security          : Enabled
- AutoLearn aging time   : 0 min
- Disableport timeout    : 20 s
- MAC move               : Denied
- Authorization fail     : Online
- NAS-ID profile is not configured
- Dot1x-failure trap     : Disabled
- Dot1x-logon trap       : Disabled
- Dot1x-logoff trap      : Enabled
- Intrusion trap         : Disabled
- Address-learned trap   : Enabled
- Mac-auth-failure trap  : Disabled
- Mac-auth-logon trap    : Enabled
- Mac-auth-logoff trap   : Disabled
- OUI value list         : 

GigabitEthernet1/0/1 is link-up
- Port mode              : macAddressElseUserLoginSecure
- NeedToKnow mode        : NeedToKnowOnly
- Intrusion protection mode : NoAction
- Security MAC address attribute
  - Learning mode         : Sticky
  - Aging type            : Periodical
- Max secure MAC addresses : 64
- Current secure MAC addresses : 0
- Authorization          : Permitted
- NAS-ID profile is not configured

# After users pass authentication, display MAC authentication information. Verify that port GigabitEthernet 1/0/1 allows multiple MAC authentication users to be authenticated.

[Device] display mac-authentication interface gigabitethernet 1/0/1

Global MAC authentication parameters:
- MAC authentication     : Enabled
- User name format       : MAC address in uppercase(XX-XX-XX-XX-XX-XX)
Username : mac
Password : Not configured
Offline detect period : 60 s
Quiet period : 5 s
Server timeout : 100 s
Authentication domain : sun
Max MAC-auth users : 2048 per slot
Online MAC-auth users : 3

Silent MAC users:

<table>
<thead>
<tr>
<th>MAC address</th>
<th>VLAN ID</th>
<th>From port</th>
<th>Port index</th>
</tr>
</thead>
</table>

GigabitEthernet1/0/1 is link-up
MAC authentication : Enabled
Authentication domain : Not configured
Auth-delay timer : Disabled
Re-auth server-unreachable : Logoff
Guest VLAN : Not configured
Guest VLAN auth-period : 30 s
Critical VLAN : Not configured
Critical voice VLAN : Disabled
Host mode : Single VLAN
Offline detection : Enabled
Authentication order : Default

Max online users : 2048
Authentication attempts : successful 3, failed 7
Current online users : 3

MAC address Auth state
1234-0300-0011 authenticated
1234-0300-0012 authenticated
1234-0300-0013 authenticated

# Display 802.1X authentication information. Verify that GigabitEthernet 1/0/1 allows only one 802.1X user to be authenticated.
[Device] display dot1x interface gigabitethernet 1/0/1

Global 802.1X parameters:
802.1X authentication : Enabled
CHAP authentication : Enabled
Max-tx period : 30 s
Handshake period : 15 s
Quiet timer : Disabled
Quiet period : 60 s
Supp timeout : 30 s
Server timeout : 100 s
Reauth period : 3600 s
Max auth requests : 2
EAD assistant function : Disabled
EAD timeout : 30 min
Domain delimiter : @
Max 802.1X users : 2048 per slot
Online 802.1X users : 1

GigabitEthernet1/0/1 is link-up
802.1X authentication : Enabled
Handshake : Enabled
Handshake reply : Disabled
Handshake security : Disabled
Unicast trigger : Disabled
Periodic reauth : Disabled
Port role : Authenticator
Authorization mode : Auto
Port access control : MAC-based
Multicast trigger : Enabled
Mandatory auth domain : Not configured
Guest VLAN : Not configured
Auth-Fail VLAN : Not configured
Critical VLAN : Not configured
Critical voice VLAN : Disabled
Re-auth server-unreachable : Logoff
Max online users : 2048
Max Attempts Fail Number : 0
Add Guest VLAN delay : Disabled

EAPOL packets: Tx 16331, Rx 102
Sent EAP Request/Identity packets : 16316
  EAP Request/Challenge packets: 6
  EAP Success packets: 4
  EAP Failure packets: 5
Received EAPOL Start packets : 6
  EAPOL LogOff packets: 2
  EAP Response/Identity packets : 80
  EAP Response/Challenge packets: 6
  Error packets: 0
Online 802.1X users: 1

# Verify that frames with an unknown destination MAC address, multicast address, or broadcast address are discarded. (Details not shown.)

Troubleshooting port security

Cannot set the port security mode

Symptom

Cannot set the port security mode for a port.
Analysis

For a port operating in a port security mode other than noRestrictions, you cannot change the port security mode by using the `port-security port-mode` command.

Solution

To resolve the problem:

1. Set the port security mode to noRestrictions.
   
   [Device-GigabitEthernet1/0/1] undo port-security port-mode

2. Set a new port security mode for the port, for example, autoLearn.
   
   [Device-GigabitEthernet1/0/1] port-security port-mode autolearn

3. If the problem persists, contact Hewlett Packard Enterprise Support.

Cannot configure secure MAC addresses

Symptom

Cannot configure secure MAC addresses.

Analysis

No secure MAC address can be configured on a port operating in a port security mode other than autoLearn.

Solution

To resolve the problem:

1. Set the port security mode to autoLearn.

   [Device-GigabitEthernet1/0/1] undo port-security port-mode
   
   [Device-GigabitEthernet1/0/1] port-security max-mac-count 64
   
   [Device-GigabitEthernet1/0/1] port-security port-mode autolearn
   
   [Device-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1

2. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring password control

Overview

Password control allows you to implement the following features:

- Manage login and super password setup, expirations, and updates for device management users.
- Control user login status based on predefined policies.

Local users are divided into two types: device management users and network access users. This feature applies only to device management users. For more information about local users, see "Configuring AAA."

Password setting

Minimum password length

You can define the minimum length of user passwords. If a user enters a password that is shorter than the minimum length, the system rejects the password.

Password composition policy

A password can be a combination of characters from the following types:

- Uppercase letters A to Z.
- Lowercase letters a to z.
- Digits 0 to 9.
- Special characters. For information about special characters, see the password-control composition command in Security Command Reference.

Depending on the system's security requirements, you can set the minimum number of character types a password must contain and the minimum number of characters for each type, as shown in Table 17.

Table 17 Password composition policy

<table>
<thead>
<tr>
<th>Password combination level</th>
<th>Minimum number of character types</th>
<th>Minimum number of characters for each type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>One</td>
<td>One</td>
</tr>
<tr>
<td>Level 2</td>
<td>Two</td>
<td>One</td>
</tr>
<tr>
<td>Level 3</td>
<td>Three</td>
<td>One</td>
</tr>
<tr>
<td>Level 4</td>
<td>Four</td>
<td>One</td>
</tr>
</tbody>
</table>

In non-FIPS mode, all the combination levels are available for a password. In FIPS mode, only the level 4 combination is available for a password.

When a user sets or changes a password, the system checks if the password meets the combination requirement. If not, the operation fails.

Password complexity checking policy

A less complicated password such as a password containing the username or repeated characters is more likely to be cracked. For higher security, you can configure a password complexity checking policy to make sure all user passwords are relatively complicated. With such a policy configured,
when a user configures a password, the system checks the complexity of the password. If the password is complexity-incompliant, the configuration will fail.

You can apply the following password complexity requirements:

- A password cannot contain the username or the reverse of the username. For example, if the username is abc, a password such as abc982 or 2cba is not complex enough.
- A character or number cannot be included three or more times consecutively. For example, password a111 is not complex enough.

**Password updating and expiration**

**Password updating**

This feature allows you to set the minimum interval at which users can change their passwords. If a user logs in to change the password but the time passed since the last change is less than this interval, the system denies the request. For example, if you set this interval to 48 hours, a user cannot change the password twice within 48 hours.

The set minimum interval is not effective when a user is prompted to change the password at the first login or after its password aging time expires.

**Password expiration**

Password expiration imposes a lifecycle on a user password. After the password expires, the user needs to change the password.

If a user enters an expired password when logging in, the system displays an error message. The user is prompted to provide a new password and to confirm it by entering it again. The new password must be valid, and the user must enter exactly the same password when confirming it.

Telnet users, SSH users, and console users can change their own passwords. The administrator must change passwords for FTP users.

**Early notice on pending password expiration**

When a user logs in, the system checks whether the password will expire in a time equal to or less than the specified notification period. If so, the system notifies the user when the password will expire and provides a choice for the user to change the password. If the user sets a new password that is complexity-compliant, the system records the new password and the setup time. If the user chooses not to change the password or the user fails to change it, the system allows the user to log in using the current password.

Telnet users, SSH users, and console users can change their own passwords. The administrator must change passwords for FTP users.

**Login with an expired password**

You can allow a user to log in a certain number of times within a specific period of time after the password expires. For example, if you set the maximum number of logins with an expired password to 3 and the time period to 15 days, a user can log in three times within 15 days after the password expires.

**Password history**

With this feature enabled, the system stores passwords that a user has used. When a user changes the password, the system checks the new password against the current password and those stored in the password history records. The new password must be different from the current one and those stored in the history records by at least four characters. The four characters must be different from one another. Otherwise, the system will display an error message, and the password will not be changed.

You can set the maximum number of history password records for the system to maintain for each user. When the number of history password records exceeds your setting, the most recent record overwrites the earliest one.
Current login passwords of device management users are not stored in the password history. This is because a device management user password is saved in cipher text and cannot be recovered to a plaintext password.

**User login control**

**First login**

With the global password control feature enabled, users must change the password at first login before they can access the system. In this situation, password changes are not subject to the minimum change interval.

**Login attempt limit**

Limiting the number of consecutive failed login attempts can effectively prevent password guessing.

Login attempt limit takes effect on FTP and VTY users. It does not take effect on the following types of users:

- Nonexistent users (users not configured on the device).
- Web users.
- Users logging in to the device through console or AUX ports.

If a user fails to use a user account to log in after making the maximum number of consecutive attempts, login attempt limit performs the following actions:

- Adds the user account and the user's IP address to the password control blacklist. This account is locked only for this user. Other users can still use this account, and the blacklisted user can use other user accounts.
- Limits the user and user account in any of the following ways:
  - Disables the user account until the account is manually removed from the password control blacklist.
  - Allows the user to continue using the user account. The user's IP address and user account are removed from the password control blacklist when the user uses this account to successfully log in to the device.
  - Disables the user account for a period of time.

The user can use the account to log in when either of the following conditions exist:
- The locking timer expires.
- The account is manually removed from the password control blacklist before the locking timer expires.

**Maximum account idle time**

You can set the maximum account idle time for user accounts. When an account is idle for this period of time since the last successful login, the account becomes invalid.

**Password not displayed in any form**

For security purposes, nothing is displayed when a user enters a password.

**Logging**

The system logs all successful password changing events and user adding events to the password control blacklist.
FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see "Configuring FIPS") and non-FIPS mode.

Password control configuration task list

The password control features can be configured in several different views, and different views support different features. The settings configured in different views or for different objects have the following application ranges:

- Settings for super passwords apply only to super passwords.
- Settings in local user view apply only to the password of the local user.
- Settings in user group view apply to the passwords of the local users in the user group if you do not configure password policies for these users in local user view.
- Global settings in system view apply to the passwords of the local users in all user groups if you do not configure password policies for these users in both local user view and user group view.

For local user passwords, the settings with a smaller application scope have higher priority.

To configure password control, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Enabling password control</td>
</tr>
<tr>
<td>(Optional.) Setting global password control parameters</td>
</tr>
<tr>
<td>(Optional.) Setting user group password control parameters</td>
</tr>
<tr>
<td>(Optional.) Setting local user password control parameters</td>
</tr>
<tr>
<td>(Optional.) Setting super password control parameters</td>
</tr>
</tbody>
</table>

Enabling password control

To successfully enable the global password control feature and allow device management users to log in to the device, the device must have sufficient storage space.

Enabling the global password control feature is the prerequisite for all password control configurations to take effect. Then, for a specific password control feature to take effect, enable this password control feature.

After the global password control feature is enabled, you cannot display the password and super password configurations for device management users by using the corresponding display commands. However, the configuration for network access user passwords can be displayed. The first password configured for device management users must contain at least four different characters.

To ensure correct function of password control, configure the device to use NTP to obtain the UTC time. After global password control is enabled, password control will record the UTC time when the password is set. The recorded UTC time might not be consistent with the actual UTC time due to power failure or device reboot. The inconsistency will cause the password expiration feature to malfunction. For information about NTP, see Network Management and Monitoring Configuration Guide.

To enable password control:
Setting global password control parameters

The password expiration time, minimum password length, and password composition policy can be configured in system view, user group view, or local user view. The password settings with a smaller application scope have higher priority. Global settings in system view apply to the passwords of the local users in all user groups if you do not configure password policies for these users in both local user view and user group view.

The `password-control login-attempt` command takes effect immediately and can affect the users already in the password control blacklist. Other password control configurations do not take effect on users that have been logged in or passwords that have been configured.

To set global password control parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong> N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the global password control feature.</td>
<td><strong>password-control enable</strong> • In non-FIPS mode, the global password control feature is disabled by default. • In FIPS mode, the global password control feature is enabled by default, and cannot be disabled.</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Enable a specific password control feature.</td>
<td>**password-control { aging</td>
</tr>
</tbody>
</table>

The password expiration time, minimum password length, and password composition policy can be configured in system view, user group view, or local user view. The password settings with a smaller application scope have higher priority. Global settings in system view apply to the passwords of the local users in all user groups if you do not configure password policies for these users in both local user view and user group view.

The `password-control login-attempt` command takes effect immediately and can affect the users already in the password control blacklist. Other password control configurations do not take effect on users that have been logged in or passwords that have been configured.

To set global password control parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong> N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Set the password expiration time.</td>
<td><strong>password-control aging</strong> aging-time The default setting is 90 days.</td>
</tr>
<tr>
<td>3.</td>
<td>Set the minimum password update interval.</td>
<td><strong>password-control update-interval</strong> interval The default setting is 24 hours.</td>
</tr>
<tr>
<td>4.</td>
<td>Set the minimum password length.</td>
<td><strong>password-control length</strong> length • In non-FIPS mode, the default setting is 10 characters. • In FIPS mode, the default length is 15 characters.</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the password composition policy.</td>
<td><strong>password-control composition</strong> type-number [ type-length type-length ] • In non-FIPS mode, by default, a password must contain at least one character type and at least one character for each type. • In FIPS mode, by default, a password must contain at least four character types and at least one character for each type.</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the password complexity checking policy.</td>
<td><strong>password-control complexity</strong> { same-character</td>
</tr>
<tr>
<td>7.</td>
<td>Set the maximum number of history password records for</td>
<td><strong>password-control history</strong> max-record-num The default setting is 4.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>each user.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Specify the maximum number of login attempts and the action to be taken when a user fails to log in after the specified number of attempts.</td>
<td>password-control login-attempt login-times [ exceed { lock</td>
<td>lock-time time</td>
</tr>
<tr>
<td>9. Set the number of days during which a user is notified of the pending password expiration.</td>
<td>password-control alert-before-expire alert-time</td>
<td>The default setting is 7 days.</td>
</tr>
<tr>
<td>10. Set the maximum number of days and maximum number of times that a user can log in after the password expires.</td>
<td>password-control expired-user-login delay delay times times</td>
<td>By default, a user can log in three times within 30 days after the password expires.</td>
</tr>
<tr>
<td>11. Set the maximum account idle time.</td>
<td>password-control idle-time idle-time login</td>
<td>The default setting is 90 days.</td>
</tr>
</tbody>
</table>

### Setting user group password control parameters

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Create a user group and enter user group view.</td>
<td>user-group group-name</td>
<td>By default, no user group exists. For information about how to configure a user group, see &quot;Configuring AAA.&quot;</td>
</tr>
<tr>
<td>3. Configure the password expiration time for the user group.</td>
<td>password-control aging aging-time</td>
<td>By default, the password expiration time of the user group equals the global password expiration time.</td>
</tr>
<tr>
<td>4. Configure the minimum password length for the user group.</td>
<td>password-control length length</td>
<td>By default, the minimum password length of the user group equals the global minimum password length.</td>
</tr>
<tr>
<td>5. Configure the password composition policy for the user group.</td>
<td>password-control composition type-number type-number [ type-length type-length ]</td>
<td>By default, the password composition policy of the user group equals the global password composition policy.</td>
</tr>
<tr>
<td>6. Configure the password complexity checking policy for the user group.</td>
<td>password-control complexity { same-character</td>
<td>user-name } check</td>
</tr>
<tr>
<td>7. Specify the maximum number of login attempts and the action to be taken when a user in the user group fails to log in after the specified number of attempts.</td>
<td>password-control login-attempt login-times [ exceed { lock</td>
<td>lock-time time</td>
</tr>
</tbody>
</table>
Setting local user password control parameters

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a device management user and enter local user view.</td>
<td>local-user user-name class manage</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the password expiration time for the local user.</td>
<td>password-control aging aging-time</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the minimum password length for the local user.</td>
<td>password-control length length</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the password composition policy for the local user.</td>
<td>password-control composition type-number type-number [ type-length type-length ]</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the password complexity checking policy for the local user.</td>
<td>password-control complexity { same-character</td>
</tr>
<tr>
<td>7.</td>
<td>Specify the maximum number of login attempts and the action to be taken for the local user when the user fails to log in after the specified number of attempts.</td>
<td>password-control login-attempt login-times [ exceed { lock</td>
</tr>
</tbody>
</table>

Setting super password control parameters

The super password allows you to obtain a temporary user role without reconnecting to the device. For more information about passwords for user roles, see Fundamentals Configuration Guide.

To set super password control parameters:
### Displaying and maintaining password control

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display password control configuration.</td>
<td><code>display password-control [ super ]</code></td>
</tr>
<tr>
<td>Display information about users in the password control blacklist.</td>
<td>`display password-control blacklist [ user-name name</td>
</tr>
<tr>
<td>Delete users from the password control blacklist.</td>
<td><code>reset password-control blacklist [ user-name name ]</code></td>
</tr>
<tr>
<td>Clear history password records.</td>
<td>`reset password-control history-record [ user-name name</td>
</tr>
</tbody>
</table>

**NOTE:**
The `reset password-control history-record` command can delete the history password records of one or all users even when the password history feature is disabled.

### Password control configuration example

**Network requirements**

Configure a global password control policy to meet the following requirements:

- A password must contain at least 16 characters.
- A password must contain at least four character types and at least four characters for each type.
- An FTP or VTY user failing to provide the correct password in two successive login attempts is permanently prohibited from logging in.
- A user can log in five times within 60 days after the password expires.
- A password expires after 30 days.
- The minimum password update interval is 36 hours.
- The maximum account idle time is 30 days.
- A password cannot contain the username or the reverse of the username.
- No character appears consecutively three or more times in a password.

Configure a super password control policy for user role **network-operator** to meet the following requirements:
- A super password must contain at least 24 characters.
- A super password must contain at least four character types and at least five characters for each type.

Configure a password control policy for the local Telnet user **test** to meet the following requirements:
- The password must contain at least 24 characters.
- The password must contain at least four character types and at least five characters for each type.
- The password for the local user expires after 20 days.

**Configuration procedure**

```bash
# Enable the password control feature globally.
<Sysname> system-view
[Sysname] password-control enable

# Disable a user account permanently if a user fails two consecutive login attempts on the user account.
[Sysname] password-control login-attempt 2 exceed lock

# Set all passwords to expire after 30 days.
[Sysname] password-control aging 30

# Globally set the minimum password length to 16 characters.
[Sysname] password-control length 16

# Set the minimum password update interval to 36 hours.
[Sysname] password-control update-interval 36

# Specify that a user can log in five times within 60 days after the password expires.
[Sysname] password-control expired-user-login delay 60 times 5

# Set the maximum account idle time to 30 days.
[Sysname] password-control login idle-time 30

# Refuse any password that contains the username or the reverse of the username.
[Sysname] password-control complexity user-name check

# Specify that no character can be included three or more times consecutively in a password.
[Sysname] password-control complexity same-character check

# Globally specify that all passwords must each contain at least four character types and at least four characters for each type.
[Sysname] password-control composition type-number 4 type-length 4

# Set the minimum super password length to 24 characters.
[Sysname] password-control super length 24

# Specify that a super password must contain at least four character types and at least five characters for each type.
```
# Configure a super password used for switching to user role network-operator as 123456789ABGFTweuix@#$%!

# Create a device management user named test.

# Set the service type of the user to Telnet.

# Set the minimum password length to 24 for the local user.

# Specify that the password of the local user must contain at least four character types and at least five characters for each type.

# Set the password for the local user to expire after 20 days.

# Configure the password of the local user in interactive mode.

Verifying the configuration

# Display the global password control configuration.

# Display the password control configuration for super passwords.
# Display the password control configuration for local user test.
<Sysname> display local-user user-name test class manage
Total 1 local users matched.

Device management user test:
  State:          Active
  Service type:   Telnet
  User group:     system
  Bind attributes:
  Authorization attributes:
    Work directory:     flash:
    User role list:     network-operator
  Password control configurations:
    Password aging:     Enabled (20 days)
    Password length:    Enabled (24 characters)
    Password composition: Enabled (4 types, 5 characters per type)
Managing public keys

Overview

This chapter describes public key management for the following asymmetric key algorithms:

- Revest-Shamir-Adleman Algorithm (RSA).
- Digital Signature Algorithm (DSA).
- Elliptic Curve Digital Signature Algorithm (ECDSA).

Many security applications, including SSH, SSL, and PKI, use asymmetric key algorithms to secure communications between two parties, as shown in Figure 74. Asymmetric key algorithms use two separate keys (one public and one private) for encryption and decryption. Symmetric key algorithms use only one key.

**Figure 74 Encryption and decryption**

![Encryption and decryption diagram]

A key owner can distribute the public key in plain text on the network but must keep the private key in privacy. It is mathematically infeasible to calculate the private key even if an attacker knows the algorithm and the public key.

The security applications use the asymmetric key algorithms for the following purposes:

- **Encryption and decryption**—Any public key receiver can use the public key to encrypt information, but only the private key owner can decrypt the information.
- **Digital signature**—The key owner uses the private key to "sign" information to be sent. The receiver decrypts the information with the sender's public key to verify information authenticity.

RSA, DSA, and ECDSA can all perform digital signature, but only RSA can perform encryption and decryption.

Asymmetric key algorithms enable secure key distribution on an insecure network. However, the security strength of an asymmetric key algorithm still depends on key size as with any symmetric key algorithm.

**FIPS compliance**

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see “Configuring FIPS”) and non-FIPS mode.

**Creating a local key pair**

When you create a local key pair, follow these guidelines:

- The key algorithm must be the same as required by the security application.
- Enter an appropriate key modulus length at prompt (see Table 18). The longer the key modulus length, the higher the security, the longer the key generation time.
If you do not assign the key pair a name, the system assigns the default name to the key pair and marks the key pair as **default**. You can also assign the default name to another key pair, but the system does not mark the key pair as **default**. The name of a key pair must be unique among all manually named key pairs that use the same key algorithm. If a name conflict occurs, the system asks whether you want to overwrite the existing key pair.

The key pairs are automatically saved and can survive system reboots.

**Table 18 A comparison of different types of key algorithms**

<table>
<thead>
<tr>
<th>Type</th>
<th>Number of key pairs</th>
<th>Modulus length</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In non-FIPS mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- One host key pair, if you specify a key pair name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- One server key pair and one host key pair, if you do not specify a key pair name. Both key pairs use their default names.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In FIPS mode: One host key pair.</td>
<td></td>
</tr>
<tr>
<td>NOTE</td>
<td>Only SSH 1.5 uses the RSA server key pair.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In non-FIPS mode: 512 to 2048 bits, 1024 bits by default. To ensure security, use a minimum of 768 bits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In FIPS mode: 2048 bits.</td>
<td></td>
</tr>
<tr>
<td>DSA</td>
<td>One host key pair.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In non-FIPS mode: 512 to 2048 bits, 1024 bits by default. To ensure security, use a minimum of 768 bits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In FIPS mode: 2048 bits.</td>
<td></td>
</tr>
<tr>
<td>ECDSA</td>
<td>One host key pair.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Release 1111: 192 bits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Release 1121 and later:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- In non-FIPS mode: 192 bits, 256 bits, 384 bits, or 521 bits.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- In FIPS mode: 256 bits, 384 bits, or 521 bits.</td>
<td></td>
</tr>
</tbody>
</table>

To create a local key pair:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Create a local key pair.</td>
<td>By default, no local key pairs exist.</td>
</tr>
</tbody>
</table>
Distributing a local host public key

You must distribute a local host public key to a peer device so the peer device can perform the following operations:

- Use the public key to encrypt information sent to the local device.
- Authenticate the digital signature signed by the local device.

To distribute a local host public key, you must first export or display the key.

- Export a host public key:
  - Export a host public to a file.
  - Export a host public key to the monitor screen, and then save it to a file.

After the key is exported to a file, transfer the file to the peer device. On the peer device, import the key from the file.

- Display a host public key.
  After the key is displayed, record the key, for example, copy it to an unformatted file. On the peer device, you must literally enter the key.

Exporting a host public key

When you export a host public key, follow these restrictions and guidelines:

- If you specify a file name in the command, the command exports the key to the specified file.
- If you do not specify a file name, the command exports the key to the monitor screen. You must manually save the exported key to a file.

To export a local host public key:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Export a local host public key.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Export an RSA host public key:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>o In non-FIPS mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>public-key local export rsa [ name key-name ] { openssh</td>
<td>ssh1</td>
</tr>
<tr>
<td></td>
<td>o In FIPS mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>public-key local export rsa [ name key-name ] { openssh</td>
<td>ssh2 } [ filename ]</td>
</tr>
<tr>
<td></td>
<td>• Export an ECDSA host public key:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>public-key local export ecdsa [ name key-name ] { openssh</td>
<td>ssh2 } [ filename ]</td>
</tr>
<tr>
<td></td>
<td>• Export a DSA host public key:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>public-key local export dsa [ name key-name ] { openssh</td>
<td>ssh2 } [ filename ]</td>
</tr>
</tbody>
</table>

The `public-key local export ecdsa` command is available in Release 1121 and later.

Displaying a host public key

Perform the following tasks in any view:
### Display local RSA public keys.
```
display public-key local rsa public [ name key-name ]
```

### Display local ECDSA public keys.
```
display public-key local ecdsa public [ name key-name ]
```

### Display local DSA public keys.
```
display public-key local dsa public [ name key-name ]
```

**NOTE:**

Do not distribute the RSA server public key `serverkey (default)` to a peer device.

### Destroying a local key pair

To avoid key compromise, destroy a local key pair and generate a new pair after any of the following conditions occurs:
- An intrusion event has occurred.
- The storage media of the device is replaced.
- Local certificate has expired. For more information about the local certificate, see "Configuring PKI."

To destroy a local key pair:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
</tr>
<tr>
<td>2.</td>
<td>Destroy a local key pair.</td>
</tr>
</tbody>
</table>

### Configuring a peer host public key

To encrypt information sent to a peer device or authenticate the digital signature of the peer device, you must configure the peer device’s public key on the local device.

You can configure the peer host public key by using the following methods:
- Import the peer host public key form a public key file (recommended).
- Manually enter (type or copy) the peer host public key.

#### Importing a peer host public key from a public key file

Before you perform this task, make sure you have exported the host public key to a file on the peer device and obtained the file from the peer device. For information about exporting a host public key, see "Exporting a host public key."

After you import the key, the system automatically converts the imported public key to a string in the Public Key Cryptography Standards (PKCS) format.

To import a peer host public key from a public key file:
### Entering a peer host public key

Before you perform this task, make sure you have displayed the key on the peer device and recorded the key. For information about displaying a host public key, see "Displaying a host public key."

Use the **display public-key local public** command to display the public key on the peer device. The format of the public key displayed in any other way might be incorrect. If the key is not in the correct format, the system discards the key and displays an error message. If the key is valid, the system saves the key.

Always import rather than enter the peer host public key if you are not sure that the device supports the format of the recorded peer host public key.

To enter a peer host public key:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify a name for the peer host public key and enter public key view.</td>
<td>public-key peer <strong>keyname</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Type or copy the key.</td>
<td>N/A</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>peer-public-key end</td>
</tr>
</tbody>
</table>

### Displaying and maintaining public keys

Execute **display** commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display local public keys.</td>
<td><strong>display public-key local</strong> { <strong>dsa</strong></td>
</tr>
<tr>
<td>Display peer host public keys.</td>
<td><strong>display public-key peer</strong> [ <strong>brief</strong></td>
</tr>
</tbody>
</table>

### Examples of public key management

#### Example for entering a peer host public key

**Network requirements**

As shown in Figure 75, to prevent illegal access, Device B authenticates Device A through a digital signature. Before configuring authentication parameters on Device B, configure the public key of Device A on Device B.
- Configure Device B to use the asymmetric key algorithm of RSA to authenticate Device A.
- Manually specify the host public key of Device A on Device B.

**Figure 75 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. **Configure Device A:**
   
   ```
   # Create local RSA key pairs with default names on Device A, and use the default modulus length 1024 bits.
   <DeviceA> system-view
   [DeviceA] public-key local create rsa
   The range of public key modulus is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   .................++++++
   ......................................++++++
   ..++++++++
   ..............++++++++
   Create the key pair successfully.
   # Display all local RSA public keys.
   [DeviceA] display public-key local rsa public
   ==============================================  
   Key name: hostkey (default)
   Key type: RSA
   Time when key pair created: 16:48:31 2011/05/12
   Key code:
   30819F300D06092A864886F70D01010105000381BD003081B92B18100DA3B90F59237347B  
   8D41B58B8F14351280139EC9111BF0D31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E  
   45DFDF51A9C7E91D818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257  
   6B7796490AF87A8C78F4A7E31F0793D8BA06FB95D54E8B9F94EB1F2D561BF66EA27DF4788  
   CB47440AF6BB25ACA50203010001
   ==============================================  
   Key name: serverkey (default)
   Key type: RSA
   Time when key pair created: 16:48:31 2011/05/12
   Key code:
   307C300D06092A864886F70D0101010500036B003068026100C9451A80F7F0A9BA1A90C7BC  
   1C02522D19A2B19F9A75D9F02219068BD7FD90FCC2AF3634EEB9FA06478DD0A1A49ACE  
   E1362A4371549ECD858A04DE46BB8E53B6AED7F1401EE88733CA3C4CED391BAE633028A  
   AC41C80A15953FB22AA30203010001
   ```

2. **Configure Device B:**
   
   ```
   # Enter the host public key of Device A in public key view. The key must be literally the same as displayed on Device A.
   ```
<DeviceB> system-view
[DeviceB] public-key peer devicea
Enter public key view. Return to system view with "peer-public-key end" command.
[DeviceB-pkey-public-key-devicea] 30819F300D6092A864886F70D010105003818D03081890
2818100DA3B9GF59237347B
[DeviceB-pkey-public-key-devicea] 8D41B58F8143512880139EC911BF9D31EB84B6B7C7A14700
27A
C8F04A827B30C2CAF79242E
[DeviceB-pkey-public-key-devicea] 45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A744
1D2
88EC54A5D31EFAE4F681257
[DeviceB-pkey-public-key-devicea] 6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F
94E
B1F2561BF66EA27DFD4788
[DeviceB-pkey-public-key-devicea] CB47440AF6BB25ACA50203010001
# Save the public key and return to system view.
[DeviceB-pkey-public-key-devicea] peer-public-key end

Verifying the configuration

# Verify that the key is the same as on Device A.
[DeviceB] display public-key peer name devicea

---------------------------------------------
Key name: devicea
Key type: RSA
Key modulus: 1024
Key code:
30819F300D6092A864886F70D010105003818D030818902818100DA3B9GF59237347B
8D41B58F8143512880139EC911BF9D31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E
45FDFF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F681257
6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
CB47440AF6BB25ACA50203010001

Example for importing a public key from a public key file

Network requirements

As shown in Figure 76, Device B authenticates Device A through a digital signature. Before configuring authentication parameters on Device B, configure the public key of Device A on Device B.

- Configure Device B to use the asymmetric key algorithm of RSA to authenticate Device A.
- Import the host public key of Device A from the public key file to Device B.

Figure 76 Network diagram

![Network Diagram](image-url)
Configuration procedure

1. Configure Device A:

# Create local RSA key pairs with default names on Device A, and use the default modulus length 1024 bits.

```bash
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.................................................................++++++
...........................................................................
.................++++++++
..................................++++++++
Create the key pair successfully.

# Display all local RSA public keys.

[DeviceA] display public-key local rsa public
```

Key name: hostkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
```bash
30819F300D06092A864886F70D0101010500381B0030819D0B18100DA3B90F59237347B
8D41B58F8143512880139EC911BFD31EB84B6B7D7A1470027AC8F04A827B30C2CAF79242E
45FDFF51A9C7E917DB818D54CB7AEF538AB26155752A7441D288EC54A5D31EFAE4F681257
6D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54EBB9F94EB1F2D561BF66EA27DFD4788
CB47440AF6BB25ACA5D203010001
```

Key name: serverkey (default)
Key type: RSA
Time when key pair created: 16:48:31 2011/05/12
Key code:
```bash
307C300D06092A864886F70D01010500036B003068026100C9451A80F7F0A9B61A90C7BC
1C02522D19A2B19F19A75D9EF0221906BB7FD90FCC2AF3634EB9FA60478D0A1A49ACE
E1362A4371549ED858A04DEE4D6BB8B8E53B6AED7F1401EE88733CA3C4C6D391BAEB63D028A
AC41C80A15953FB22AA30203010001
```

# Export the RSA host public key to the file devicea.pub.

[DeviceA] public-key local export rsa ssh2 devicea.pub
[DeviceA] quit

# Enable the FTP server function, create an FTP user with the username ftp and password 123, and configure the FTP user role as network-admin.

[DeviceA] ftp server enable
[DeviceA] local-user ftp
[DeviceA-username-manage-ftp] password simple 123
[DeviceA-username-manage-ftp] service-type ftp
[DeviceA-username-manage-ftp] authorization-attribute user-role network-admin
[DeviceA-username-manage-ftp] quit
2. Configure Device B:

   # Use FTP in binary mode to get the public key file `devicea.pub` from Device A.
   
   `<DeviceB> ftp 10.1.1.1
   Connected to 10.1.1.1 (10.1.1.1).
   220 FTP service ready.
   User(10.1.1.1:(none)):ftp
   331 Password required for ftp.
   Password:
   230 User logged in.
   Remote system type is UNIX.
   Using binary mode to transfer files.
   ftp> binary
   200 TYPE is now 8-bit binary
   ftp> get devicea.pub
   227 Entering Passive Mode (10,1,1,118,252)
   150 Accepted data connection
   226 File successfully transferred
   301 bytes received in 0.003 seconds (98.0 kbyte/s)
   ftp> quit
   221-Goodbye. You uploaded 0 and downloaded 1 kbytes.
   221 Logout.

   # Import the host public key from the key file `devicea.pub`.
   
   `<DeviceB> system-view
   [DeviceB] public-key peer devicea import sshkey devicea.pub
   
   Verifying the configuration
   
   # Verify that the host public key is the same as it is on Device A.
   
   `[DeviceB] display public-key peer name devicea
   `---------------------------------------------
   Key name: devicea
   Key type: RSA
   Key modulus: 1024
   Key code: 30819F300D06092A864886F70D0101010003818D00030818902818100DA3B90F59237347B8D41B58F8143512880139EC9111BFD31EB84B6B7C7A1470027AC8F04A827B30C2CAF79242E45FDF51A9C7E917DB818D54CB7AEF538AB261557524A7441D288EC54A5D31EFAE4F6812576D7796490AF87A8C78F4A7E31F0793D8BA06FB95D54ED6B9F94EB1F2D561BF66EA27D7DF4788CB47440AF6BB25ACA50203010001
   `---------------------------------------------
Configuring PKI

Overview

Public Key Infrastructure (PKI) is an asymmetric key infrastructure to encrypt and decrypt data for securing network services. Data encrypted with the public key can be decrypted only with the private key. Likewise, data encrypted with the private key can be decrypted only with the public key.

PKI uses digital certificates to distribute and employ public keys, and provides network communication and e-commerce with security services such as user authentication, data confidentiality, and data integrity.

Hewlett Packard Enterprise's PKI system provides certificate management for IPsec and SSL.

PKI terminology

Digital certificate

A digital certificate is an electronic document signed by a CA that binds a public key with the identity of its owner.

A digital certificate includes the following information:

- Issuer name (the name of the CA that issued the certificate).
- Subject name (name of the individual or group to which the certificate is issued).
- Identity information of the subject.
- Subject's public key.
- Signature of the CA.
- Period of validity.

A digital certificate must comply with the international standards of ITU-T X.509, of which X.509 v3 is the most commonly used.

This chapter covers the following types of certificates:

- **CA certificate**—Certificate of a CA. Multiple CAs in a PKI system form a CA tree, with the root CA at the top. The root CA generates a self-signed certificate, and each lower level CA holds a CA certificate issued by the CA immediately above it. The chain of these certificates forms a chain of trust.

- **Registration authority (RA) certificate**—Certificate issued by a CA to an RA. RAs act as proxies for CAs to process enrollment requests in a PKI system.

- **Local certificate**—Digital certificate issued by a CA to a PKI entity, which contains the entity's public key.

- **Peer certificate**—Digital certificate of a peer, which contains the peer's public key and is signed by a CA.

Certificate revocation list

A certificate revocation list (CRL) is a list of serial numbers for certificates that have been revoked. A CRL is created and signed by the CA that originally issued the certificates.

The CA publishes CRLs periodically to revoke certificates. Entities that are associated with the revoked certificates should not be trusted.

The CA must revoke a certificate when any of the following conditions occurs:

- The certificate subject name is changed.
• The private key is compromised.
• The association between the subject and CA is changed. For example, when an employee terminates employment with an organization.

**CA policy**

A CA policy is a set of criteria that a CA follows to process certificate requests, to issue and revoke certificates, and to publish CRLs. Typically, a CA advertises its policy in a certification practice statement (CPS). You can obtain a CA policy through out-of-band means such as phone, disk, and email. Make sure you understand the CA policy before you select a trusted CA for certificate request because different CAs might use different policies.

**PKI architecture**

A PKI system consists of PKI entities, CAs, RAs and a certificate/CRL repository, as shown in Figure 77.

**Figure 77 PKI architecture**

- **PKI entity**—An end user using PKI certificates. The PKI entity can be an operator, an organization, a device like a router or a switch, or a process running on a computer. PKI entities use SCEP to communicate with the CA or RA.
- **CA**—Certification authority that grants and manages certificates. A CA issues certificates, defines the certificate validity periods, and revokes certificates by publishing CRLs.
- **RA**—Registration authority, which offloads the CA by processing enrollment requests. The RA accepts certificate requests, verifies user identity, and determines whether to ask the CA to issue certificates.

The RA is optional in a PKI system. In cases when the CA operates over a wide geographical area or when there is security concern over exposing the CA to direct network access, it is advisable to delegate some of the tasks to an RA and leave the CA to concentrate on its primary tasks of signing certificates and CRLs.

- **Certificate/CRL repository**—A certificate distribution point that stores certificates and CRLs, and distributes these certificates and CRLs to PKI entities. It also provides the query function. A PKI repository can be a directory server using the LDAP or HTTP protocol, of which LDAP is commonly used.

**PKI operation**

The following workflow describes how a PKI entity requests a local certificate from a CA that has RAs:
1. A PKI entity submits a certificate request to the RA.
2. The RA verifies the identity of the entity and sends a digital signature containing the identity information and the public key to the CA.
3. The CA verifies the digital signature, approves the request, and issues a certificate.
4. After receiving the certificate from the CA, the RA sends the certificate to the certificate repositories and notifies the PKI entity that the certificate has been issued.
5. The entity obtains the certificate from the certificate repository.

PKI applications

The PKI technology can meet security requirements of online transactions. As an infrastructure, PKI has a wide range of applications. Here are some application examples.

- **VPN**—A VPN is a private data communication network built on the public communication infrastructure. A VPN can use network layer security protocols (for example, IPsec) in conjunction with PKI-based encryption and digital signature technologies for confidentiality.

- **Secure emails**—PKI can address the email requirements for confidentiality, integrity, authentication, and non-repudiation. A common secure email protocol is Secure/Multipurpose Internet Mail Extensions (S/MIME), which is based on PKI and allows for transfer of encrypted mails with signature.

- **Web security**—PKI can be used in the SSL handshake phase to verify the identities of the communicating parties by digital certificates.

Support for MPLS L3VPN

An enterprise might have multiple branches in different VPNs. PKI support for MPLS L3VPN is required if users in different VPNs request certificates from the CA server in the headquarters VPN.

As shown in Figure 78, the PKI entity in VPN 1 requests a certificate from the CA server in VPN 3 in the following workflow:

1. The PKI entity submits a certificate request to the CA server.
2. The PE device that connects to the PKI entity transmits the request to the CA server through MPLS L3VPN.
3. The CA server verifies the request and issues the certificate.
4. The PE device that connects to the CA server transmits the certificate to the PKI entity.

For information about MPLS L3VPN, see *MPLS Configuration Guide*.

Figure 78 PKI support for MPLS L3VPN
FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see “Configuring FIPS”) and non-FIPS mode.

PKI configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring a PKI entity</td>
</tr>
<tr>
<td>(Required.) Configuring a PKI domain</td>
</tr>
<tr>
<td>(Required.) Requesting a certificate:</td>
</tr>
<tr>
<td>• Configuring automatic certificate request</td>
</tr>
<tr>
<td>• Manually requesting a certificate</td>
</tr>
<tr>
<td>(Optional.) Aborting a certificate request</td>
</tr>
<tr>
<td>(Optional.) Obtaining certificates</td>
</tr>
<tr>
<td>(Optional.) Verifying PKI certificates</td>
</tr>
<tr>
<td>(Optional.) Specifying the storage path for the certificates and CRLs</td>
</tr>
<tr>
<td>(Optional.) Exporting certificates</td>
</tr>
<tr>
<td>(Optional.) Removing a certificate</td>
</tr>
<tr>
<td>(Optional.) Configuring a certificate-based access control policy</td>
</tr>
</tbody>
</table>

Configuring a PKI entity

A certificate applicant uses an entity to provide its identity information to a CA. A valid PKI entity must include one or more of the following identity categories:

- Distinguished name (DN) of the entity, which further includes the common name, county code, locality, organization, unit in the organization, and state. If you configure the DN for an entity, a common name is required.
- FQDN of the entity.
- IP address of the entity.

Whether the categories are required or optional depends on the CA policy. Follow the CA policy to configure the entity settings. For example, if the CA policy requires the entity DN, but you configure only the IP address, the CA rejects the certificate request from the entity.

The SCEP add-on on the Windows 2000 CA server has restrictions on the data length of a certificate request. If a request from a PKI entity exceeds the data length limit, the CA server does not respond to the certificate request. In this case, you can use an out-of-band means to submit the request. Other types of CA servers, such as RSA servers and OpenCA servers, do not have such restrictions.

To configure a PKI entity:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Create a PKI entity and enter its view.</td>
<td>pki entity entity-name</td>
<td>By default, no PKI entities exist.</td>
</tr>
</tbody>
</table>
### Configuring a PKI domain

A PKI domain contains enrollment information for a PKI entity. It is locally significant and is intended only for reference by other applications like IKE and SSL.

To configure a PKI domain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a PKI domain and enter its view.</td>
<td>pki domain domain-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the trusted CA.</td>
<td>ca identifier name</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the PKI entity name.</td>
<td>certificate request entity entity-name</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the type of certificate request reception authority.</td>
<td>certificate request from { ca</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the certificate request URL.</td>
<td>certificate request url url-string [ vpn-instance vpn-instance-name ]</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>7.</td>
<td>certificate request polling { count count</td>
<td>interval minutes }</td>
</tr>
<tr>
<td>8.</td>
<td>ldap-server host hostname [ port port-number ] [ vpn-instance vpn-instance-name ]</td>
<td>This task is required only when the CRL repository is an LDAP server and the URL of the CRL repository does not contain the host name of the LDAP server. By default, no LDAP server is specified.</td>
</tr>
<tr>
<td>9.</td>
<td>root-certificate fingerprint { md5</td>
<td>sha1 } string</td>
</tr>
<tr>
<td>10.</td>
<td>public-key rsa { { encryption name encryption-key-name [ length key-length ]</td>
<td>signature name signature-key-name [ length key-length ] } *</td>
</tr>
<tr>
<td>11.</td>
<td>usage { ike</td>
<td>ssl-client</td>
</tr>
</tbody>
</table>
12. (Optional.) Specify a source IP address for the PKI protocol packets.

- Specify the source IPv4 address for the PKI protocol packets: `source ip { ip-address | interface (interface-type interface-number) }
- Specify the source IPv6 address for the PKI protocol packets: `source ipv6 { ipv6-address | interface { interface-type interface-number } }

This task is required if the CA policy requires that the CA server accept certificate requests from a specific IP address or subnet. By default, the source IP address of PKI protocol packets is the IP address of their outgoing interface.

### Requesting a certificate

To request a certificate, a PKI entity must provide its identity information and public key to a CA.

A certificate request can be submitted to a CA in offline or online mode.

- **Offline mode**—A certificate request is submitted by using an out-of-band method, such as phone, disk, or email. You can use this mode as required or if you fail to request a certificate in online mode.

  To submit a certificate request in offline mode:
  a. Use `pki request-certificate domain pkcs10` to print the request information on the terminal or use `pki request-certificate domain pkcs10 filename` to save the request information to a local file.
  b. Send the printed information or the saved file to the CA by using an out-of-band method to submit the request.

- **Online mode**—A certificate request can be automatically or manually submitted. This section describes the online request mode.

### Configuration guidelines

The following guidelines apply to certificate request for an entity in a PKI domain:

- Make sure the device is time synchronized with the CA server. Otherwise, the certificate request might fail because the certificate is considered to be outside of the validity period. For information about how to configure the system time, see *Fundamentals Configuration Guide*.

- To request a new certificate for a PKI entity that already has a local certificate, perform the following steps:
  a. Use the `pki delete-certificate` command to delete the existing local certificate.
  b. Use the `public-key local create` to generate a new key pair. The new key pair will automatically overwrite the old key pair in the domain.
  c. Submit a new certificate request.

- After a new certificate is obtained, do not use the `public-key local create` or `public-key local destroy` command to generate or destroy a key pair with the same name as the key pair in the local certificate. Otherwise, the existing local certificate becomes unavailable.

- A PKI domain can have local certificates using only one type of cryptographic algorithms (RSA, DSA, or ECDSA). If DSA or ECDSA is used, a PKI domain can have only one local certificate. If RSA is used, a PKI domain can have one local certificate for signature, and one local certificate for encryption.
Configuring automatic certificate request

**IMPORTANT:**
The device does not support automatic certificate rollover. To avoid service interruptions, you must manually submit a certificate renewal request before the current certificate expires.

In auto request mode, a PKI entity automatically submits a certificate request to the CA when an application works with the PKI entity that does not have a local certificate. For example, when IKE negotiation uses a digital signature for identity authentication, but no local certificate is available, the entity automatically submits a certificate request. It saves the certificate locally after obtaining it from the CA.

A CA certificate must be present before you request a local certificate. If no CA certificate exists in the PKI domain, the PKI entity automatically obtains a CA certificate before sending a certificate request.

To configure automatic certificate request:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter PKI domain view.</td>
<td>pki domain domain-name</td>
</tr>
<tr>
<td>3.</td>
<td>Set the certificate request mode to auto.</td>
<td>certificate request mode auto [ password { cipher</td>
</tr>
</tbody>
</table>

Manually requesting a certificate

Before you manually submit a certificate request, make sure the CA certificate exists and a key pair is specified for the PKI domain:

- The CA certificate is used to verify the authenticity and validity of the obtained local certificate.
- The key pair is used for certificate request. Upon receiving the public key and the identity information, the CA signs and issues a certificate.

After the CA issues the certificate, the device obtains and saves it locally.

To manually request a certificate:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter PKI domain view.</td>
<td>pki domain domain-name</td>
</tr>
<tr>
<td>3.</td>
<td>Set the certificate request mode to manual.</td>
<td>certificate request mode manual</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Obtain the CA certificate.</td>
<td>See &quot;Obtaining certificates.&quot;</td>
</tr>
<tr>
<td>6.</td>
<td>Submit a certificate request or generate a certificate request in PKCS#10 format.</td>
<td>pki request-certificate domain domain-name [ password password ] [ pkcs10 [ filename filename ] ]</td>
</tr>
</tbody>
</table>
## Aborting a certificate request

Before the CA issues a certificate, you can abort a certificate request and change its parameters, such as the common name, country code, or FQDN. You can use the `display pki certificate request-status` command to display the status of a certificate request.

Alternatively, you also can remove a PKI domain to abort the associated certificate request.

To abort a certificate request:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Abort a certificate request.</td>
<td>pki abort-certificate-request domain domain-name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This command is not saved in the configuration file.</td>
</tr>
</tbody>
</table>

## Obtaining certificates

You can obtain the CA certificate, local certificates, and peer certificates related to a PKI domain from a CA and save them locally for higher lookup efficiency. To do so, use either the offline mode or the online mode:

- In offline mode, obtain the certificates by an out-of-band means like FTP, disk, or email, and then import them locally. Use this mode when the CRL repository is not specified, the CA server does not support SCEP, or the CA server generates the key pair for the certificates.
- In online mode, you can obtain the CA certificate through SCEP and obtain local certificates or peer certificates through LDAP.

## Configuration prerequisites

To obtain local or peer certificates in online mode, specify the LDAP server for the PKI domain.

To import local or peer certificates in offline mode, perform the following tasks:

- Use FTP or TFTP to upload the certificate files to the storage media of the device. If FTP or TFTP is not available, display and copy the contents of a certificate to a file on the device. Make sure the certificate is in PEM format because only certificates in PEM format can be imported.
- To import a certificate, a CA certificate chain must exist in the PKI domain, or be contained in the certificate. If the CA certificate chain is not available, obtain it before importing the certificate.

## Configuration guidelines

- To import a local certificate containing an encrypted key pair, you must provide the challenge password. Contact the CA administrator to obtain the password.
• If a CA certificate already exists locally, you cannot obtain it again in online mode. If you want to obtain a new one, use the `pki delete-certificate` command to remove the existing CA certificate and local certificates first.

• If local or peer certificates already exist, you can obtain new local or peer certificates to overwrite the existing ones. If RSA is used, a PKI domain can have two local certificates, one for signature and the other for encryption.

• If CRL checking is enabled, obtaining a certificate triggers CRL checking. If the certificate to be obtained has been revoked, the certificate cannot be obtained.

• The device compares the validity period of a certificate with the local system time to determine whether the certificate is valid. Make sure the system time of the device is synchronized with the CA server.

### Configuration procedure

To obtain certificates:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Obtain certificates.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Import certificates in offline mode: `pki import domain domain-name { der ( ca</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Obtain certificates in online mode: `pki retrieve-certificate domain domain-name { ca</td>
</tr>
</tbody>
</table>

### Verifying PKI certificates

A certificate is automatically verified when it is requested, obtained, or used by an application. If the certificate expires, if it is not issued by a trusted CA, or if it is revoked, the certificate cannot be used.

You can also manually verify a certificate. If it has been revoked, the certificate cannot be requested or obtained.

### Verifying certificates with CRL checking

CRL checking checks whether a certificate is in the CRL. If it is, the certificate has been revoked and its home entity is not trusted.

To use CRL checking, a CRL must be obtained from a CRL repository. The device selects a CRL repository in the following order:

1. CRL repository specified in the PKI domain by using this command.
2. CRL repository in the certificate that is being verified.
3. CRL repository in the CA certificate or CRL repository in the upper-level CA certificate if the CA certificate is the certificate being verified.

If no CRL repository is found after the selection process, the device obtains the CRL through SCEP. In this scenario, the CA certificate and the local certificates must have been obtained.

To verify certificates with CRL checking:
### Verifying certificates without CRL checking

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter PKI domain view.</td>
<td>pki domain domain-name</td>
<td>N/A</td>
</tr>
<tr>
<td>3. Disable CRL checking.</td>
<td>undo crl check enable</td>
<td>By default, CRL checking is enabled.</td>
</tr>
<tr>
<td>4. Return to system view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>5. Obtain the CA certificate.</td>
<td>See &quot;Obtaining certificates.&quot;</td>
<td>N/A</td>
</tr>
<tr>
<td>6. Verify the validity of the certificates.</td>
<td>pki validate-certificate domain domain-name { ca</td>
<td>local }</td>
</tr>
</tbody>
</table>

### Specifying the storage path for the certificates and CRLs

⚠️ **CAUTION:**

If you change the storage path, save the configuration before you reboot or shut down the device to avoid loss of the certificates or the CRLs.

The device has a default storage path for certificates and CRLs. You can change the storage path and specify different paths for the certificates and CRLs.
After you change the storage path for certificates or CRLs, the certificate files (with the .cer or .p12 extension) and CRL files (with the .crl extension) in the original path are moved to the new path.

To specify the storage path for the certificates and CRLs:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the storage path for certificates and CRLs.</td>
<td>pki storage { certificates</td>
<td>By default, the device stores certificates and CRLs in the PKI directory on the storage media of the device.</td>
</tr>
<tr>
<td></td>
<td>crls } dir-path</td>
<td></td>
</tr>
</tbody>
</table>

### Exporting certificates

**IMPORTANT:**

To export all certificates in the PKCS12 format, the PKI domain must have a minimum of one local certificate. Otherwise, the certificates in the PKI domain cannot be exported.

You can export the CA certificate and the local certificates in a PKI domain to certificate files. The exported certificate files can then be imported back to the device or other PKI applications.

When you export a local certificate with the RSA key pair, the name of the target file might not be the same as specified in the command. It depends on the purpose of the key pair of the certificate.

To export certificates:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Export certificates.</td>
<td>• Export certificates in DER format: pki export domain domain-name der ( all</td>
<td>If you do not specify a file name when you export a certificate in PEM format, the certificate is displayed on the terminal.</td>
</tr>
<tr>
<td></td>
<td>ca</td>
<td>local ) filename filename</td>
</tr>
<tr>
<td></td>
<td>• Export certificates in PKCS12 format: pki export domain domain-name p12 ( all</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>local ) passphrase p12passwordstring</td>
</tr>
<tr>
<td></td>
<td>• Export certificates in PEM format: pki export domain domain-name pem</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>( { all</td>
</tr>
<tr>
<td></td>
<td></td>
<td>filename</td>
</tr>
</tbody>
</table>

### Removing a certificate

You can remove the CA certificate, local certificate, or peer certificates in a PKI domain. After you remove the CA certificate, the system automatically removes the local certificates, peer certificates, and CRLs in the domain.

You can remove a local certificate and request a new one when the local certificate is about to expire or the certificate's private key is compromised. To remove a local certificate and request a new certificate, perform the following tasks:

1. Remove the local certificate.
2. Use the **public-key local destroy** command to destroy the existing local key pair.
3. Use the **public-key local create** command to generate a new key pair.
4. Request a new certificate.
To remove a certificate:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Remove a certificate.</td>
<td>pki delete-certificate domain domain-name { ca</td>
</tr>
</tbody>
</table>

Configuring a certificate-based access control policy

Certificate-based access control policies allow you to authorize access to a device (for example, an HTTPS server) based on the attributes of an authenticated client’s certificate.

A certificate-based access control policy is a set of access control rules (permit or deny statements), each associated with a certificate attribute group. A certificate attribute group contains multiple attribute rules, each defining a matching criterion for an attribute in the certificate issuer name, subject name, or alternative subject name field.

If a certificate matches all attribute rules in a certificate attribute group associated with an access control rule, the system determines that the certificate matches the access control rule. In this scenario, the match process stops, and the system performs the access control action defined in the access control rule.

The following conditions describe how a certificate-based access control policy verifies the validity of a certificate:

- If a certificate matches a permit statement, the certificate passes the verification.
- If a certificate matches a deny statement or does not match any statements in the policy, the certificate is regarded invalid.
- If a statement is associated with a non-existing attribute group, or the attribute group does not have attribute rules, the certificate matches the statement.
- If the certificate-based access control policy referenced by a security application (for example, HTTPS) does not exist, all certificates in the application pass the verification.

To configure a certificate-based access control policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a certificate attribute group and enter its view.</td>
<td>pki certificate attribute-group group-name</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Configure an attribute rule for issuer name, subject name, or alternative subject name.</td>
<td>attribute id { alt-subject-name ( fqdn</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Create a certificate-based access control policy and enter its view.</td>
<td>pki certificate access-control-policy policy-name</td>
</tr>
</tbody>
</table>
### Displaying and maintaining PKI

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the contents of a certificate.</td>
<td>`display pki certificate domain domain-name { ca</td>
</tr>
<tr>
<td>Display certificate request status.</td>
<td><code>display pki certificate request-status [ domain domain-name ]</code></td>
</tr>
<tr>
<td>Display locally stored CRLs in a PKI domain.</td>
<td><code>display pki crl domain domain-name</code></td>
</tr>
<tr>
<td>Display certificate attribute group information.</td>
<td><code>display pki certificate attribute-group [ group-name ]</code></td>
</tr>
<tr>
<td>Display certificate-based access control policy information.</td>
<td><code>display pki certificate access-control-policy [ policy-name ]</code></td>
</tr>
</tbody>
</table>

#### PKI configuration examples

You can use different software applications, such as Windows server, RSA Keon, and OpenCA, to act as the CA server.

If you use Windows server or OpenCA, you must install the SCEP add-on for Windows server or enable SCEP for OpenCA. In either case, when you configure a PKI domain, you must use the `certificate request from ra` command to specify the RA to accept certificate requests.

If you use RSA Keon, the SCEP add-on is not required. When you configure a PKI domain, you must use the `certificate request from ca` command to specify the CA to accept certificate requests.

#### Requesting a certificate from an RSA Keon CA server

**Network requirements**

Configure the PKI entity (the device) to request a local certificate from the CA server.

**Figure 79 Network diagram**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>Create a certificate access control rule.</td>
<td>By default, no certificate access control rules are configured, and all certificates can pass the verification. You can create multiple access control rules for a certificate-based access control policy.</td>
</tr>
</tbody>
</table>
Configuring the RSA Keon CA server

1. Create a CA server named myca:
   In this example, you must configure these basic attributes on the CA server:
   o **Nickname**—Name of the trusted CA.
   o **Subject DN**—DN attributes of the CA, including the common name (CN), organization unit (OU), organization (O), and country (C).
   You can use the default values for other attributes.

2. Configure extended attributes:
   Configure parameters in the Jurisdiction Configuration section on the management page of the CA server:
   o Select the correct extension profiles.
   o Enable the SCEP autovetting function to enable the CA server to automatically approve certificate requests without manual intervention.
   o Specify the IP address list for SCEP autovetting.

Configuring the device

1. Synchronize the system time of the device with the CA server for the device to correctly request certificates or obtain CRLs. (Details not shown.)

2. Create an entity named aaa and set the common name to Device.

   ```
   <Device> system-view
   [Device] pki entity aaa
   [Device-pki-entity-aaa] common-name Device
   [Device-pki-entity-aaa] quit
   ```

3. Configure a PKI domain:
   # Create a PKI domain named torsa and enter its view.
   ```
   [Device] pki domain torsa
   ```
   # Specify the name of the trusted CA as myca.
   ```
   [Device-pki-domain-torsa] ca identifier myca
   ```
   # Specify the URL of the CA server. The URL format is http://host:port/Issuing Jurisdiction ID, where Issuing Jurisdiction ID is a hexadecimal string generated on the CA server.
   ```
   [Device-pki-domain-torsa] certificate request url
   http://1.1.2.22:446/80f6214aa8865301d07929ae481c7ceed99f95bd
   ```
   # Specify the CA for accepting certificate requests.
   ```
   [Device-pki-domain-torsa] certificate request from ca
   ```
   # Specify the PKI entity name as aaa.
   ```
   [Device-pki-domain-torsa] certificate request entity aaa
   ```
   # Specify the URL of the CRL repository.
   ```
   [Device-pki-domain-torsa] crl url ldap://1.1.2.22:389/CN=myca
   ```
   # Specify the RSA key pair with the purpose `general`, the name `abc`, and the length 1024 bits.
   ```
   [Device-pki-domain-torsa] public-key rsa general name abc length 1024
   [Device-pki-domain-torsa] quit
   ```

4. Generate a local RSA key pair.
   ```
   [Device] public-key local create rsa name abc
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   ```
Create the key pair successfully.

5. Request a local certificate:

   # Obtain the CA certificate and save it locally.
   [Device] pki retrieve-certificate domain torsa ca
   The trusted CA's finger print is:
     MD5 fingerprint: EDE9 0394 A273 B61A F1B3 0072 A0B1 F9A8
     SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8
   Is the finger print correct?(Y/N): y
   Retrieved the certificates successfully.

   # Submit a certificate request manually. You must specify a password for certificate revocation when an RSA Keon CA server is used.
   [Device] pki request-certificate domain torsa password 1111
   Start to request the general certificate ...
       
   Certificate requested successfully.

Verifying the configuration

   # Display information about the local certificate in PKI domain torsa.
   [Device] display pki certificate domain torsa local
   Certificate:
       Data:
         Version: 3 (0x2)
         Serial Number:
         Signature Algorithm: sha1WithRSAEncryption
         Issuer: CN=myca
         Validity
           Not Before: Jan 6 03:10:58 2013 GMT
           Not After : Jan 6 03:10:58 2014 GMT
         Subject: CN=Device
         Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
             Public-Key: (1024 bit)
               Modulus:
                 00:ab:45:64:a8:6c:10:70:3b:b9:46:34:8d:eb:1a:
                 3a:5a:64:0c:8f:93:e5:f0:70:67:dc:cd:c1:6f:7a:
                 7e:f8:18:30:f6:6b:00:d6:50:48:23:5c:8c:05:30:
                 f1:9c:22:be:f3:1b:37:73:44:f5:2d:2c:5e:8f:40:
                 3e:36:36:0d:c8:33:90:f3:9b
               Exponent: 65537 (0x10001)
         X509v3 extensions:
           X509v3 CRL Distribution Points:
Full Name: DirName: CN = myca

Signature Algorithm: sha1WithRSAEncryption
25:90:4a:8e:c6:cc:b8:1a:fa:e0:bc:17:e0:6a:11:ae:e7:36:
1b:f5

To display detailed information about the CA certificate, use the display pki certificate domain command.

Requesting a certificate from a Windows Server 2003 CA server

Network requirements

Configure the PKI entity (the device) to request a local certificate from a Windows Server 2003 CA server.

Figure 80 Network diagram

Configuring the Windows Server 2003 CA server

1. Install the certificate service component:
   a. Select Control Panel > Add or Remove Programs from the start menu.
   c. Click Next to begin the installation.
   d. Set the CA name. In this example, set the CA name to myca.

2. Install the SCEP add-on:
   By default, Windows Server 2003 does not support SCEP. You must install the SCEP add-on on the server for a PKI entity to register and obtain a certificate from the server. After the SCEP add-on installation is complete, you will see a URL. Specify this URL as the certificate request URL on the device.

3. Modify the certificate service attributes:
   a. Select Control Panel > Administrative Tools > Certificate Authority from the start menu.
      If the certificate service component and SCEP add-on have been installed successfully, there should be two certificates issued by the CA to the RA.
   b. Right-click the CA server in the navigation tree and select Properties > Policy Module.
   c. Click Properties and then select Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.

4. Modify the Internet information services attributes:
a. Select Control Panel > Administrative Tools > Internet Information Services (IIS) Manager from the start menu.

b. Select Web Sites from the navigation tree.


d. Specify the path for certificate service in the Local path box.

e. Specify a unique port number for the default website to avoid conflict with existing services. In this example, port 8080 is used.

Configuring the device

1. Synchronize the device’s system time with the CA server for the device to correctly request certificates. (Details not shown.)

2. Create an entity named aaa and set the common name to test.

   <Device> system-view
   [Device] pki entity aaa
   [Device-pki-entity-aaa] common-name test
   [Device-pki-entity-aaa] quit

3. Configure a PKI domain:

   # Create a PKI domain named winserver and enter its view.
   [Device] pki domain winserver
   # Set the name of the trusted CA to myca.
   [Device-pki-domain-winserver] ca identifier myca
   # Configure the certificate request URL. The URL format is http://host:port/certsrv/mscep/mscep.dll, where host:port is the host IP address and port number of the CA server.
   [Device-pki-domain-winserver] certificate request url http://4.4.4.1:8080/certsrv/mscep/mscep.dll
   # Specify the RA to accept certificate requests.
   [Device-pki-domain-winserver] certificate request from ra
   # Specify the PKI entity name as aaa.
   [Device-pki-domain-winserver] certificate request entity aaa
   # Specify the RSA key pair with the purpose general, the name abc, and the length 1024 bits.
   [Device-pki-domain-winserver] public-key rsa general name abc length 1024
   [Device-pki-domain-winserver] quit

4. Generate an RSA local key pair:

   [Device] public-key local create rsa name abc
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   .........................++++++
   .....................................++++++
   Create the key pair successfully.

5. Request a local certificate:

   # Obtain the CA certificate and save it locally.
   [Device] pki retrieve-certificate domain winserver ca
   The trusted CA's fingerprint is:
   MD5 fingerprint: 766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB
SHA1 fingerprint: 97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4
Is the fingerprint correct? (Y/N): y
Retrieved the certificates successfully.

# Submit a certificate request manually.
[Device] pki request-certificate domain winserver
Start to request the general certificate ...

Certificate requested successfully.

Verifying the configuration

# Display information about the local certificate in PKI domain winserver.
[Device] display pki certificate domain winserver local
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        (Negative) 01:03:99:ff:ff:ff:fd:11
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: CN=sec
    Validity
        Not Before: Dec 24 07:09:42 2012 GMT
        Not After : Dec 24 07:19:42 2013 GMT
    Subject: CN=test
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            dc:31:41:3f:5d:5b:36:9e:53:dc:3a:bc:0d:11:fb:
            9c:ca:0b:01:5e:8d:2e:91:89:2f:11:e3:1e:12:8a:
            ee:60:83:b3:d3:e5:e8:e5:02:cf:b0:e8:f0:3a:a4:
            b7:aca:02:2c:4d:47:5f:39:4b:2c:87:ff:2e:ea:ad:
            25:39
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Key Usage:
            Digital Signature, Non Repudiation, Key Encipherment, Data Encip
X509v3 Subject Key Identifier:
X509v3 Authority Key Identifier:
B

X509v3 CRL Distribution Points:

Full Name:
  URI:file://\g07904c\CertEnroll\sec.crl

Authority Information Access:
  CA Issuers - URI:http://gc/CertEnroll/gc_sec.crt
  CA Issuers - URI:file://\gc\CertEnroll\gc_sec.crt

1.3.6.1.4.1.311.20.2:
  .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
Signature Algorithm: sha1WithRSAEncryption
  02:09:ad:08

To display detailed information about the CA certificate, use the display pki certificate domain command.

**Requesting a certificate from an OpenCA server**

**Network requirements**

Configure the PKI entity (the device) to request a local certificate from the CA server.

**Figure 81 Network diagram**
Configuring the OpenCA server

The configuration is not shown. For information about how to configure an OpenCA server, see related manuals.

When you configure the CA server, use the OpenCA version later than version 0.9.2 because the earlier versions do not support SCEP.

Configuring the device

1. Synchronize the device's system time with the CA server for the device to correctly request certificates. (Details not shown.)

2. Create an entity named aaa with the common name as rnd, the country code as CN, the organization name as test, and the unit name as software.

   <Device> system-view
   [Device] pki entity aaa
   [Device-pki-entity-aaa] common-name rnd
   [Device-pki-entity-aaa] country CN
   [Device-pki-entity-aaa] organization test
   [Device-pki-entity-aaa] organization-unit software
   [Device-pki-entity-aaa] quit

3. Configure a PKI domain:

   # Create a PKI domain named openca and enter its view.
   [Device] pki domain openca
   # Specify the name of the trusted CA as myca.
   [Device-pki-domain-openca] ca identifier myca
   # Configure the certificate request URL. The URL is in the format http://host/cgi-bin/pki/scep, where host is the host IP address of the OpenCA server.
   [Device-pki-domain-openca] certificate request url http://192.168.222.218/cgi-bin/pki/scep
   # Configure the device to send certificate requests to ra.
   [Device-pki-domain-openca] certificate request from ra
   # Specify the PKI entity name as aaa.
   [Device-pki-domain-openca] certificate request entity aaa
   # Specify the RSA key pair with the purpose general, the name abc, and the length 1024 bits.
   [Device-pki-domain-openca] public-key rsa general name abc length 1024
   [Device-pki-domain-openca] quit

4. Generate a local RSA key pair.

   [Device] public-key local create rsa name abc
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   .................................................................+++++
   .................................................................+++++
   Create the key pair successfully.

5. Request a local certificate:

   # Obtain the CA certificate and save it locally.
   [Device] pki retrieve-certificate domain openca ca
   The trusted CA's finger print is:
MD5 fingerprint: 5AA3 DEFD 7B23 2A25 16A3 14F4 C81C C0FA
SHA1 fingerprint: 9E68 4E63 D742 4B09 90E0 4C78 E213 F15F DC8E 9122

Is the fingerprint correct? (Y/N): y
Retrieved the certificates successfully.

# Submit a certificate request manually.
[Device] pki request-certificate domain openca
Start to request the general certificate ...

Certificate requested successfully.

Verifying the configuration

# Display information about the local certificate in PKI domain openca.
[Device] display pki certificate domain openca local
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=CN, L=shangdi ST=pukras, O=OpenCA Labs, OU=mysubUnit, CN=sub-ca, DC=pki-subdomain, DC=mydomain-sub, DC=com
Validity
Not Before: Jun 30 09:09:09 2011 GMT
Not After : May 1 09:09:09 2012 GMT
Subject: CN=rnd, O=test, OU=software, C=CN
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Modulus:
00:b8:7a:9a:b8:59:eb:fc:70:3e:bf:19:54:0c:7e:
59:46:2b:ec:0d:21:1d:00:05:8a:bf:ee:ac:61:03:
6c:1f:35:b5:b4:cd:86:9f:45
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Cert Type:
SSL Client, S/MIME
X509v3 Key Usage:
Digital Signature, Non Repudiation, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
Netscape Comment:

User Certificate of OpenCA Labs

X509v3 Subject Key Identifier:

X509v3 Authority Key Identifier:

X509v3 Issuer Alternative Name:
DNS:root@docm.com, DNS:, IP Address:192.168.154.145, IP Address:192.168.154.138

Authority Information Access:
CA Issuers - URI:http://192.168.222.218/pki/pub/cacert/cacert.crt
1.3.6.1.5.5.7.48.12 - URI:http://192.168.222.218:830/

X509v3 CRL Distribution Points:

Full Name:
URI:http://192.168.222.218/pki/pub/crl/cacrl.crl

Signature Algorithm: sha256WithRSAEncryption
81:99:31:89

To display detailed information about the CA certificate, use the display pki certificate domain command.

Certificate import and export configuration example

Network requirements

As shown in Figure 82, Device B will replace Device A in the network. The PKI domain exportdomain on Device A has two local certificates containing the private key and one CA certificate. To make sure the certificates are still valid after Device B replaces Device A, copy the certificates on Device A to Device B and follow these guidelines:

- Encrypt the private key in the local certificates using 3DES_CBC with the password 111111 when you export the local certificates from Device A.
- Save the certificates on Device A in PEM format to the PKI domain importdomain on Device B.
Configuration procedure

1. Export the certificate on Device A to specified files:
   # Export the CA certificate to a .pem file.
   `<DeviceA> system-view
   [DeviceA] pki export domain exportdomain pem ca filename pkicachain.pem
   # Export the local certificate to a file named pkilocal.pem in PEM format, and use 3DES_CBC to encrypt the private key with the password 111111.
   [DeviceA] pki export domain exportdomain pem local 3des-cbc 111111 filename pkilocal.pem

   After the previous operations, the system generates three certificate files in PEM format: a CA certificate file and two local certificate files. The CA certificate file is named `pkicachain.pem`. The two local certificate files are named `pkilocal.pem-signature` and `pkilocal.pem-encryption`, and contain the private key for signature and encryption, respectively.

   # Display the local certificate file `pkilocal.pem-signature`.
   `<DeviceA> quit
   <DeviceA> more pkicachain.pem-sign
   Bag Attributes
   friendlyName: 
   localKeyID: 90 C6 DC 1D 20 49 4F 24 70 F5 17 17 20 2B 9E AC 20 F3 99 89
   subject=/C=CN/O=OpenCA Labs/OU=Users/CN=subsign 11
   issuer=/C=CN/L=shangdi/ST=pukras/O=OpenCA Labs/OU=docm/CN=subcal
   -----BEGIN CERTIFICATE-----
   MIIEgjCCA2qgAwIBAgILAJgsebpejZc5UwAwDQYJKoZIhvcNAQELBQAwZjELMAkG
   ...
friendlyName:
   localKeyID: D5 DF 29 28 C8 B9 D9 49 4B C2 BC 66 75 FE D6 6C C8
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=subencr 11
issuer=/C=CN/L=shangdi/ST=pukras/O=OpenCA Labs/OU=docm/CN=subcal
-----BEGIN CERTIFICATE-----
MIIEUDCCAzigAwIBAgIKCHxnAVyzWhIPLzANBgkqhkiG9w0BAQsFADBmMQswCQYD
-----END CERTIFICATE-----
Bag Attributes
   friendlyName:
   localKeyID: D5 DF 29 28 C8 B9 D9 49 4B C2 BC 66 75 FE D6 6C C8
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICxjBABgkqhkiG9w0BBQwMzAbBgkqhkiG9w0BBQwwDgQI7H0mb407/GACAggA
-----END ENCRYPTED PRIVATE KEY-----

2. Download the certificate files pkicachain.pem, pkilocal.pem-sign, and pkilocal.pem-encr from Device A to the host through FTP. (Details not shown.)

3. Upload the certificate files pkicachain.pem, pkilocal.pem-sign, and pkilocal.pem-encr from the host to Device B through FTP. (Details not shown.)

4. Import the certificate files to Device B:
   # Disable CRL checking. (You can configure CRL checking as required. This example assumes CRL checking is not required.)
   <DeviceB> system-view
   [DeviceB] pki domain importdomain
   [DeviceB-pki-domain-importdomain] undo crl check enable
   # Specify the RSA key pair for signature as sign, and the RSA key pair for encryption as encr for certificate request.
   [DeviceB-pki-domain-importdomain] public-key rsa signature name sign encryption name encr
   [DeviceB-pki-domain-importdomain] quit
   # Import the CA certificate file pkicachain.pem in PEM format to the PKI domain.
   [DeviceB] pki import domain importdomain pem ca filename pkicachain.pem
   # Import the local certificate file pkilocal.pem-signature in PEM format to the PKI domain. The certificate file contains a key pair.
   [DeviceB] pki import domain importdomain pem local filename pkilocal.pem-signature
   Please input the password:******
   # Import the local certificate file pkilocal.pem-encryption in PEM format to the PKI domain. The certificate file contains a key pair.
   [DeviceB] pki import domain importdomain pem local filename pkilocal.pem-encryption
   Please input the password:******
   # Display the imported local certificate information on Device B.
   [DeviceB] display pki certificate domain importdomain local Certificate:
   Data:
   Version: 3 (0x2)
   Serial Number:
   98:2c:79:ba:5e:8d:97:39:53:00
   Signature Algorithm: sha256WithRSAEncryption

250
Issuer: C=CN, L=shangdi, ST=pukras, O=OpenCA Labs, OU=docm, CN=subcal

Validity
Not Before: May 26 05:56:49 2011 GMT
Not After : Nov 22 05:56:49 2012 GMT

Subject: C=CN, O=OpenCA Labs, OU=Users, CN=subsign 11

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)
Modulus:
ce:8d:6a:4c:3a:30:19:3c:14:ff:a9:50:04:f5:00:

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:
CA:FALSE

Netscape Cert Type:
SSL Client, S/MIME

X509v3 Key Usage:
Digital Signature, Non Repudiation

X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection, Microsoft 
Smartcardlogin

Netscape Comment:
User Certificate of OpenCA Labs

X509v3 Subject Key Identifier:

X509v3 Authority Key Identifier:

X509v3 Subject Alternative Name:
email:subsign@docm.com

X509v3 Issuer Alternative Name:
DNS:subca1@docm.com, DNS:, IP Address:1.1.2.2, IP Address:2.2.1.1

Authority Information Access:
CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
OCSP - URI:http://titan:2560/
1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

X509v3 CRL Distribution Points:

Full Name:
URI:http://192.168.40.130/pki/pub/crl/cacrl.crl
Signature Algorithm: sha256WithRSAEncryption
d6:0a:1c:0b

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 08:7c:67:01:5c:b3:5a:12:0f:2f
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=CN, L=shangdi, ST=pukras, O=OpenCA Labs, OU=docm, CN=subca1

Validity
Not Before: May 26 05:58:26 2011 GMT
Not After : Nov 22 05:58:26 2012 GMT
Subject: C=CN, O=OpenCA Labs, OU=Users, CN=subencr 11
Subject Public Key Info:
Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)
Modulus:
8c:2e:00:d1:e9:a4:5b:18:39
Exponent: 65537 (0x10001)

X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Cert Type:
    SSL Server
X509v3 Key Usage:
  Key Encipherment, Data Encipherment

Netscape Comment:
  Server of OpenCA Labs

X509v3 Subject Key Identifier:

X509v3 Authority Key Identifier:

X509v3 Subject Alternative Name:
  email:subencr@docm.com

X509v3 Issuer Alternative Name:
  DNS:subca1@docm.com, DNS:, IP Address:1.1.2.2, IP Address:2.2.1.1

Authority Information Access:
  CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
  OCSP - URI:http://titan:2560/
  1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

X509v3 CRL Distribution Points:
  Full Name:
  URI:http://192.168.40.130/pki/pub/crl/cacrl.crl

Signature Algorithm: sha256WithRSAEncryption
  79:05:cd:c3

To display detailed information about the CA certificate, use the **display pki certificate domain** command.

**Troubleshooting PKI configuration**

This section provides troubleshooting information for common problems with PKI.
Failed to obtain the CA certificate

Symptom
The CA certificate cannot be obtained.

Analysis
- The network connection is down, for example, because the network cable is damaged or the connectors have bad contact.
- No trusted CA is specified.
- The certificate request URL is incorrect or not specified.
- The system time of the device is not synchronized with the CA server.
- The source IP address of the PKI protocol packets is not specified or not correct.
- The fingerprint of the root CA certificate is illegal.

Solution
1. Check for and fix any network connection problems.
2. Verify that the required configurations are correct.
3. Use ping to verify that the CA or RA is accessible from the specified certificate request URL.
4. Synchronize the system time of the device with the CA server.
5. Specify the correct source IP address for PKI protocol packets that the CA server can accept.
6. Verify the CA certificate’s fingerprint on the CA server.
7. If the problem persists, contact Hewlett Packard Enterprise Support.

Failed to obtain local certificates

Symptom
No local certificates can be obtained.

Analysis
- The network connection is down.
- No CA certificate has been obtained before you try to obtain local certificates.
- The LDAP server is not configured or is incorrectly configured.
- No key pair is specified for the PKI domain for certificate request, or the specified key pair does not match the local certificates to the obtained.
- The PKI domain does not reference the PKI entity configuration, or the PKI entity configuration is incorrect.
- CRL checking is enabled, but CRLs do not exist locally or CRLs cannot be obtained.
- The CA server does not accept the source IP address specified in the PKI domain, or the source IP address is incorrect.
- The system time of the device is not synchronized with the CA server.

Solution
1. Check for and fix any network connection problems.
2. Obtain or import the CA certificate.
3. Configure the correct LDAP server.
4. Specify the key pair used for certificate request in the PKI domain, or remove the existing key pair and submit a certificate request again.
5. Check the registration policy on the CR or RA, and make sure the attributes of the PKI entity meet the policy requirements.
6. Obtain the CRL from the CRL repository.
7. Specify the correct source IP address that the CA server can accept. For the correct settings, contact the CA administrator.
8. Synchronize the system time of the device with the CA server.
9. If the problem persists, contact Hewlett Packard Enterprise Support.

Failed to request local certificates

Symptom
Local certificate requests cannot be submitted.

Analysis
- The network connection is down, for example, because the network cable is damaged or the connectors have bad contact.
- No CA certificate has been obtained before you submit the certificate request.
- The certificate request URL is incorrect or is not specified.
- The certificate request reception authority is incorrect or is not specified.
- The required parameters are not configured for the PKI entity or are mistakenly configured.
- No key pair is specified for the PKI domain for certificate request, or the key pair is changed during a certificate request process.
- Exclusive certificate request applications are running in the PKI domain.
- The PKI domain is not specified with the source IP address of the PKI protocol packets that the CA server can accept, or is specified with an incorrect one.
- The system time of the device is not synchronized with the CA server.

Solution
1. Check for and fix any network connection problems.
2. Obtain or import the CA certificate.
3. Use ping to verify that the CA or RA is accessible from the specified certificate request URL.
4. Specify the correct certificate request URL.
5. Check the registration policy on the CR/RA, and make sure the attributes of the PKI entity meet the policy requirements.
6. Specify the key pair used for certificate request in the PKI domain, or remove the key pair specified in the PKI and submit a certificate request again.
7. Use pki abort-certificate-request domain to abort the certificate request.
8. Specify the correct source IP address that the CA server can accept. For the correct settings, contact the CA administrator.
9. Synchronize the system time of the device with the CA server.
10. If the problem persists, contact Hewlett Packard Enterprise Support.

Failed to obtain CRLs

Symptom
CRLs cannot be obtained.
Analysis

- The network connection is down, for example, because the network cable is damaged or the connectors have bad contact.
- No CA certificate has been obtained before you try to obtain CRLs.
- The URL of the CRL repository is not configured and cannot be obtained from the CA certificate or local certificates in the PKI domain.
- The specified URL of the CRL repository is incorrect.
- The device tries to obtain CRLs through SCEP, but experiences the following problems:
  - The PKI domain does not have local certificates.
  - The key pairs in the certificates have been changed.
  - The PKI domain has incorrect URL for certificate request.
- The specified URL of the CRL repository does not contain the host name or IP address, and the LDAP server is incorrect or is not specified in the PKI domain.
- The CA does not issue CRLs.
- The PKI domain is not specified with the source IP address that the CA server can accept, or is specified with an incorrect one.

Solution

1. Check for and fix any network connection problems.
2. Obtain or import the CA certificate.
3. If the URL of the CRL repository cannot be obtained, verify that the following conditions exist:
   - The URL for certificate request is valid.
   - A local certificate has been successfully obtained.
   - The local certificate contains a public key that matches the locally stored key pair.
4. Make sure the LDAP server address is contained in the CRL repository URL, or is configured in the PKI domain.
5. Make sure the CA server support publishing CRLs.
6. Specify a correct source IP address that the CA server can accept. For the correct settings, contact the CA administrator.
7. If the problem persists, contact Hewlett Packard Enterprise Support.

Failed to import the CA certificate

Symptom

The CA certificate cannot be imported.

Analysis

- CRL checking is enabled, but the device does not have a locally stored CRL and cannot obtain one.
- The specified format does not match the actual format of the file to be imported.

Solution

1. Use `undo crl check enable` to disable CRL checking.
2. Make sure the format of the imported file is correct.
3. If the problem persists, contact Hewlett Packard Enterprise Support.
Failed to import a local certificate

Symptom
A local certificate cannot be imported.

Analysis
- The PKI domain does not have a locally stored CA certificate, and the certificate file to be imported does not contain the CA certificate chain.
- CRL checking is enabled, but the device does not have a locally stored CRL and cannot obtain one.
- The specified format does not match the actual format of the file to be imported.
- The device and the certificate do not have the local key pair.
- The certificate has been revoked.
- The certificate is out of the validity period.
- The system time is wrong.

Solution
1. Obtain or import the CA certificate.
2. Use `undo crl check enable` to disable CRL checking, or obtain the CRL before you import certificates.
3. Make sure the format of the file to be imported is correct.
4. Make sure the certificate file contains the private key.
5. Make sure the certificate is not revoked.
6. Make sure the certificate is within the validity period.
7. Configure the correct system time for the device.
8. If the problem persists, contact Hewlett Packard Enterprise Support.

Failed to export certificates

Symptom
Certificates cannot be exported.

Analysis
- The PKI domain does not have local certificates when you export all certificates in PKCS12 format.
- The specified export path does not exist.
- The specified export path is invalid.
- The public key of the local certificate to be exported does not match the public key in the key pair of the PKI domain.
- The storage space of the device is full.

Solution
1. Obtain or request local certificates.
2. Use `mkdir` to create the required path.
3. Specify a correct export path.
4. Configure the correct key pair in the PKI domain.
5. Clear up the storage space of the device.
6. If the problem persists, contact Hewlett Packard Enterprise Support.

Failed to set the storage path

**Symptom**

The storage path for certificates or CRLs cannot be set.

**Analysis**

- The specified storage path does not exist.
- The specified storage path is illegal.
- The storage space of the device is full.

**Solution**

1. Use `mkdir` to create the path.
2. Specify a valid storage path for certificates or CRLs.
3. Clear up the storage space of the device.
4. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring IPsec

The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see Layer 2—LAN Switching Configuration Guide).

⚠ **CAUTION:**
- If you configure both IPsec and QoS on an interface, make sure the IPsec traffic classification rules match the QoS traffic classification rules. If the rules do not match, QoS might classify the packets of one IPsec SA to different queues, causing packets to be sent out of order. When IPsec anti-replay is enabled, IPsec will drop the incoming packets that are out of the anti-replay window, resulting in packet loss. IPsec traffic classification rules are determined by the specified ACL rules. For information about QoS classification rules, see ACL and QoS Configuration Guide.
- ACLs for IPsec take effect only on traffic that is generated by the device and traffic that is destined for the device. They do not take effect on traffic forwarded through the device.

Overview

IP Security (IPsec) is defined by the IETF to provide interoperable, high-quality, cryptographically-based security for IP communications. It is a Layer 3 VPN technology that transmits data in a secure channel established between two endpoints (such as two security gateways). Such a secure channel is usually called an IPsec tunnel.

IPsec is a security framework that has the following protocols and algorithms:
- Authentication Header (AH).
- Encapsulating Security Payload (ESP).
- Internet Key Exchange (IKE).
- Algorithms for authentication and encryption.

AH and ESP are security protocols that provide security services. IKE performs automatic key exchange. For more information about IKE, see "Configuring IKE."

IPsec provides the following security services for data packets in the IP layer:
- **Confidentiality**—The sender encrypts packets before transmitting them over the Internet, protecting the packets from being eavesdropped en route.
- **Data integrity**—The receiver verifies the packets received from the sender to make sure they are not tampered with during transmission.
- **Data origin authentication**—The receiver verifies the authenticity of the sender.
- **Anti-replay**—The receiver examines packets and drops outdated and duplicate packets.

IPsec delivers the following benefits:
- Reduced key negotiation overhead and simplified maintenance by supporting the IKE protocol. IKE provides automatic key negotiation and automatic IPsec security association (SA) setup and maintenance.
- Good compatibility. You can apply IPsec to all IP-based application systems and services without modifying them.
- Encryption on a per-packet rather than per-flow basis. Per-packet encryption allows for flexibility and greatly enhances IP security.
Security protocols and encapsulation modes

Security protocols

IPsec comes with two security protocols, AH and ESP. They define how to encapsulate IP packets and the security services that they can provide.

- **AH** (protocol 51) defines the encapsulation of the AH header in an IP packet, as shown in Figure 85. AH can provide data origin authentication, data integrity, and anti-replay services to prevent data tampering, but it cannot prevent eavesdropping. Therefore, it is suitable for transmitting non-confidential data. AH supports authentication algorithms HMAC-MD5 and HMAC-SHA1.

- **ESP** (protocol 50) defines the encapsulation of the ESP header and trailer in an IP packet, as shown in Figure 85. ESP can provide data encryption, data origin authentication, data integrity, and anti-replay services. Unlike AH, ESP can guarantee data confidentiality because it can encrypt the data before encapsulating the data to IP packets. ESP supports encryption algorithms such as DES, 3DES, and AES, and authentication algorithms HMAC-MD5 and HMAC-SHA1.

Both AH and ESP provide authentication services, but the authentication service provided by AH is stronger. In practice, you can choose either or both security protocols. When both AH and ESP are used, an IP packet is encapsulated first by ESP and then by AH.

Encapsulation modes

IPsec supports the following encapsulation modes:

- **Transport mode**—The security protocols protect the upper layer data of an IP packet. Only the transport layer data is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are placed after the original IP header. You can use the transport mode when end-to-end security protection is required (the secured transmission start and end points are the actual start and end points of the data). The transport mode is typically used for protecting host-to-host communications, as shown in Figure 83.

  ![Figure 83 IPsec protection in transport mode](image)

- **Tunnel mode**—The security protocols protect the entire IP packet. The entire IP packet is used to calculate the security protocol headers. The calculated security protocol headers and the encrypted data (only for ESP encapsulation) are encapsulated in a new IP packet. In this mode, the encapsulated packet has two IP headers. The outer IP header is added by the network device that provides the IPsec service. You must use the tunnel mode when the secured transmission start and end points are not the actual start and end points of the data packets (for example, when two gateways provide IPsec but the data start and end points are two hosts behind the gateways). The tunnel mode is typically used for protecting gateway-to-gateway communications, as shown in Figure 84.

  ![Figure 84 IPsec protection in tunnel mode](image)
A security association (SA) is an agreement negotiated between two communicating parties called IPsec peers. An SA comprises the following parameters for data protection:

- Security protocols (AH, ESP, or both).
- Encapsulation mode (transport mode or tunnel mode).
- Authentication algorithm (HMAC-MD5 or HMAC-SHA1).
- Encryption algorithm (DES, 3DES, or AES).
- Shared keys and their lifetimes.

An SA is unidirectional. At least two SAs are needed to protect data flows in a bidirectional communication. If two peers want to use both AH and ESP to protect data flows between them, they construct an independent SA for each protocol in each direction.

An SA is uniquely identified by a triplet, which consists of the security parameter index (SPI), destination IP address, and security protocol identifier. An SPI is a 32-bit number that identifies an SA. It is transmitted in the AH/ESP header.

An SA can be set up manually or through IKE.

- **Manual mode**—Configure all parameters for the SA through commands. This configuration mode is complex and does not support some advanced features (such as periodic key update), but it can implement IPsec without IKE. This mode is mainly used in small and static networks or when the number of IPsec peers in the network is small.

- **IKE negotiation mode**—The peers negotiate and maintain the SA through IKE. This configuration mode is simple and has good expansibility. As a best practice, set up SAs through IKE negotiations in medium- and large-scale dynamic networks.

A manually configured SA never ages out. An IKE-created SA has a lifetime, which comes in two types:

- **Time-based lifetime**—Defines how long the SA can be valid after it is created.
- **Traffic-based lifetime**—Defines the maximum traffic that the SA can process.

If both lifetime timers are configured for an SA, the SA becomes invalid when either of the lifetime timers expires. Before the SA expires, IKE negotiates a new SA, which takes over immediately after its creation.
Authentication and encryption

Authentication algorithms

IPsec uses hash algorithms to perform authentication. A hash algorithm produces a fixed-length digest for an arbitrary-length message. IPsec peers respectively calculate message digests for each packet. The receiver compares the local digest with that received from the sender. If the digests are identical, the receiver considers the packet intact and the sender's identity valid. IPsec uses the Hash-based Message Authentication Code (HMAC) based authentication algorithms, including HMAC-MD5 and HMAC-SHA1. Compared with HMAC-SHA1, HMAC-MD5 is faster but less secure.

Encryption algorithms

IPsec uses symmetric encryption algorithms, which encrypt and decrypt data by using the same keys. The following encryption algorithms are available for IPsec on the device:

- **DES**—Encrypts a 64-bit plaintext block with a 56-bit key. DES is the least secure but the fastest algorithm.
- **3DES**—Encrypts plaintext data with three 56-bit DES keys. The key length totals up to 168 bits. It provides moderate security strength and is slower than DES.
- **AES**—Encrypts plaintext data with a 128-bit, 192-bit, or 256-bit key. AES provides the highest security strength and is slower than 3DES.

IPsec implementation

To implement IPsec protection for packets between two peers, complete the following tasks on each peer:

- Configure an IPsec policy, which defines the range of packets to be protected by IPsec and the security parameters used for the protection.
- Apply the IPsec policy to an interface or an application.

When you apply an IPsec policy to an interface, you implement IPsec based on the interface. Packets received and sent by the interface are protected according to the IPsec policy. When you apply an IPsec policy to an application, you implement IPsec based on the application. Packets of the application are protected according to the IPsec policy, regardless of the receiving and sending interface of the packets.

IPsec protects packets as follows:

- When an IPsec peer identifies the packets to be protected according to the IPsec policy, it sets up an IPsec tunnel and sends the packet to the remote peer through the tunnel. The IPsec tunnel can be manually configured beforehand, or it can be set up through IKE negotiation triggered by the packet. The IPsec tunnels are actually the IPsec SAs. The inbound packets are protected by the inbound SA, and the outbound packets are protected by the outbound SA.
- When the remote IPsec peer receives the packet, it drops, de-encapsulates, or directly forwards the packet according to the configured IPsec policy.

Interface-based IPsec supports setting up IPsec tunnels based on ACLs.

ACL-based IPsec

To implement ACL-based IPsec, configure an ACL to define the data flows to be protected, specify the ACL in an IPsec policy, and then apply the IPsec policy to an interface. When packets sent by the interface match the permit rule of the ACL, the packets are protected by the outbound IPsec SA and encapsulated with IPsec. When the interface receives an IPsec packet whose destination address is the IP address of the local device, it searches for the inbound IPsec SA according to the SPI carried in the IPsec packet header for de-encapsulation. If the de-encapsulated packet matches the permit rule of the ACL, the device processes the packet. Otherwise, it drops the packet.

The device supports the following data flow protection modes:
• **Standard mode**—One IPsec tunnel protects one data flow. The data flow permitted by an ACL rule is protected by one IPsec tunnel that is established solely for it.

• **Aggregation mode**—One IPsec tunnel protects all data flows permitted by all the rules of an ACL. This mode is only used to communicate with old-version devices.

• **Per-host mode**—One IPsec tunnel protects one host-to-host data flow. One host-to-host data flow is identified by one ACL rule and protected by one IPsec tunnel established solely for it. This mode consumes more system resources when multiple data flows exist between two subnets to be protected.

**Application-based IPsec**

This IPsec implementation method does not require any ACL. All packets of the application bound to an IPsec policy are encapsulated with IPsec, and all packets of the applications that are not bound with IPsec and the IPsec packets that failed to be de-encapsulated are dropped.

You can use IPsec to protect an IPv6 routing protocol by using this method. The supported IPv6 routing protocols include OSPFv3, IPv6 BGP, and RIPv6.

In one-to-many communication scenarios, you must configure the IPsec SAs for an IPv6 routing protocol in manual mode because of the following reasons:

- The automatic key exchange mechanism is only used to protect communications between two points. In one-to-many communication scenarios, automatic key exchange cannot be implemented.

- One-to-many communication scenarios require that all the devices use the same SA parameters (SPI and key) to receive and send packets. IKE negotiated SAs cannot meet this requirement.

**Protocols and standards**

- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2402, *IP Authentication Header*
- RFC 2406, *IP Encapsulating Security Payload*
- RFC 4552, *Authentication/Confidentiality for OSPFv3*

**FIPS compliance**

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see "Configuring FIPS") and non-FIPS mode.

**IPsec tunnel establishment**

IPsec tunnels can be established in different methods. Choose a correct method to establish IPsec tunnels according to your network conditions:

- **ACL-based IPsec tunnel**—Protects packets identified by an ACL. To establish an ACL-based IPsec tunnel, configure an IPsec policy, specify an ACL in the policy, and apply the policy to an interface (see "Implementing ACL-based IPsec"). The IPsec tunnel establishment steps are the same in an IPv4 network and in an IPv6 network.

- **Application-based IPsec tunnel**—Protects the packets of an application. This method can be used to protect IPv6 routing protocols. It does not require any ACL. To establish application-based IPsec tunnels, configure manual IPsec profiles and bind the profiles to an IPv6 routing protocol. For more information about IPv6 routing protocols, see "Configuring IPsec for IPv6 routing protocols."
Implementing ACL-based IPsec

Feature restrictions and guidelines

ACLs for IPsec take effect only on traffic that is generated by the device and traffic that is destined for the device. They do not take effect on traffic forwarded through the device. For example, an ACL-based IPsec tunnel can protect log messages the device sends to a log server, but it cannot protect all the data flows and voice flows that are forwarded by the device. For more information about configuring an ACL for IPsec, see "Configuring an ACL."

Typically, IKE uses UDP port 500 for communication, and AH and ESP use the protocol numbers 51 and 50. Make sure traffic of these protocols is not denied on the interfaces with IKE or IPsec configured.

ACL-based IPsec configuration task list

The generic configuration procedure for implementing ACL-based IPsec is as follows:

1. Configure an ACL for identifying data flows to be protected. To use IPsec to protect VPN traffic, you do not need to specify the VPN parameters in the ACL rules.
2. Configure IPsec transform sets to specify the security protocols, authentication and encryption algorithms, and the encapsulation mode.
3. Configure an IPsec policy to associate data flows with the IPsec transform sets, specify the SA negotiation mode, the peer IP addresses (the start and end points of the IPsec tunnel), the required keys, and the SA lifetime.
   An IPsec policy is a set of IPsec policy entries that have the same name but different sequence numbers. In the same IPsec policy, an IPsec policy entry with a smaller sequence number has a higher priority.
4. Apply the IPsec policy to an interface.

Complete the following tasks to configure ACL-based IPsec:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Conﬁguring an ACL</td>
</tr>
<tr>
<td>(Required.) Conﬁguring an IPsec transform set</td>
</tr>
<tr>
<td>(Required.) Conﬁgure an IPsec policy (use either method):</td>
</tr>
<tr>
<td>• Conﬁguring a manual IPsec policy</td>
</tr>
<tr>
<td>• Conﬁguring an IKE-based IPsec policy</td>
</tr>
<tr>
<td>(Required.) Applying an IPsec policy to an interface</td>
</tr>
<tr>
<td>(Optional.) Enabling ACL checking for de-encapsulated packets</td>
</tr>
<tr>
<td>(Optional.) Conﬁguring IPsec anti-replay</td>
</tr>
<tr>
<td>(Optional.) Conﬁguring IPsec anti-replay redundancy</td>
</tr>
<tr>
<td>(Optional.) Binding a source interface to an IPsec policy</td>
</tr>
<tr>
<td>(Optional.) Enabling QoS pre-classify</td>
</tr>
<tr>
<td>(Optional.) Enabling logging of IPsec packets</td>
</tr>
<tr>
<td>(Optional.) Conﬁguring the DF bit of IPsec packets</td>
</tr>
<tr>
<td>(Optional.) Conﬁguring SNMP notifications for IPsec</td>
</tr>
</tbody>
</table>
Configuring an ACL

IPsec uses ACLs to identify the traffic to be protected.

Keywords in ACL rules

An ACL is a collection of ACL rules. Each ACL rule is a deny or permit statement. A permit statement identifies a data flow protected by IPsec, and a deny statement identifies a data flow that is not protected by IPsec. With IPsec, a packet is matched against the ACL rules and processed according to the first rule that it matches:

- Each ACL rule matches both the outbound traffic and the returned inbound traffic.
- In the outbound direction, if a permit statement is matched, IPsec considers that the packet requires protection and continues to process it. If a deny statement is matched or no match is found, IPsec considers that the packet does not require protection and delivers it to the next module.
- In the inbound direction:
  - Non-IPsec packets that match a permit statement are dropped.
  - IPsec packets that match a permit statement and are destined for the device itself are de-encapsulated. By default, the device matches the de-encapsulated packets against the ACL again and, if they match a permit statement, continues to process the packets. If ACL checking for de-encapsulated packets is disabled, the device directly processes the de-encapsulated packets without matching against the ACL.

When defining ACL rules for IPsec, follow these guidelines:

- Permit only data flows that need to be protected and use the any keyword with caution. With the any keyword specified in a permit statement, all outbound traffic matching the permit statement will be protected by IPsec. All inbound IPsec packets matching the permit statement will be received and processed, but all inbound non-IPsec packets will be dropped. This will cause all the inbound traffic that does not need IPsec protection to be dropped.
- Avoid statement conflicts in the scope of IPsec policy entries. When creating a deny statement, be careful with its matching scope and matching order relative to permit statements. The policy entries in an IPsec policy have different match priorities. ACL rule conflicts between them are prone to cause mistreatment of packets. For example, when configuring a permit statement for an IPsec policy entry to protect an outbound traffic flow, you must avoid the situation that the traffic flow matches a deny statement in a higher priority IPsec policy entry. Otherwise, the packets will be sent out as normal packets. If they match a permit statement at the receiving end, they will be dropped by IPsec.

Mirror image ACLs

To make sure SAs can be set up and the traffic protected by IPsec can be processed correctly between two IPsec peers, create mirror image ACLs on the IPsec peers.

Configuring an IPsec transform set

An IPsec transform set, part of an IPsec policy, defines the security parameters for IPsec SA negotiation, including the security protocol, encryption algorithms, and authentication algorithms.

Changes to an IPsec transform set affect only SAs negotiated after the changes. To apply the changes to existing SAs, execute the reset ipsec sa command to clear the SAs so that they can be set up by using the updated parameters.

To configure an IPsec transform set:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2. Create an IPsec transform set and enter its view.</td>
<td><code>ipsec transform-set transform-set-name</code></td>
<td>By default, no IPsec transform set exists.</td>
</tr>
<tr>
<td>3. Specify the security protocol for the IPsec transform set.</td>
<td>`protocol { ah</td>
<td>ah-esp</td>
</tr>
</tbody>
</table>

(Release 1111.) Specify the encryption algorithm for ESP:
- In non-FIPS mode:
  `esp encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des-cbc | null }` *
- In FIPS mode:
  `esp encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 }` *

(Release 1121 and later.) Specify the encryption algorithm for ESP:
- In non-FIPS mode:
- In FIPS mode:

(Release 1111.) Specify the authentication algorithm for ESP:
- In non-FIPS mode:
  `esp authentication-algorithm { md5 | sha1 }` *
- In FIPS mode:
  `esp authentication-algorithm sha1`

(Release 1121 and later.) Specify the authentication algorithm for ESP:
- In non-FIPS mode:
  `esp authentication-algorithm { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512 }` *
- In FIPS mode:
  `esp authentication-algorithm { sha1 | sha256 | sha384 | sha512 }` *

(Release 1111.) Specify the encryption algorithm for ESP:
- In non-FIPS mode:
  `esp encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des-cbc | null }` *
- In FIPS mode:

(Release 1111.) Specify the authentication algorithm for ESP:
- In non-FIPS mode:
  `esp authentication-algorithm { md5 | sha1 | sha256 | sha384 | sha512 }` *
- In FIPS mode:
  `esp authentication-algorithm { sha1 | sha256 | sha384 | sha512 }` *

Configure at least one command. By default, no security algorithm is specified.

You can specify security algorithms for a security protocol only when the security protocol is used by the transform set. For example, you can specify the ESP-specific security algorithms only when you select ESP or AH-ESP as the security protocol.

If you use ESP in FIPS mode, you must specify both the ESP encryption algorithm and the ESP authentication algorithm.

You can specify multiple algorithms by using one command, and the algorithm specified earlier has a higher priority.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication algorithm for AH:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• In non-FIPS mode:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ah authentication-algorithm (md5</td>
<td>sha1 ) *</td>
<td></td>
</tr>
<tr>
<td>• In FIPS mode:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ah authentication-algorithm sha1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Release 1121 and later.) Specify the authentication algorithm for AH:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• In non-FIPS mode:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ah authentication-algorithm { aes-xcbc-mac</td>
<td>md5</td>
<td>sha1</td>
</tr>
<tr>
<td>• In FIPS mode:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ah authentication-algorithm { sha1</td>
<td>sha256</td>
<td>sha384</td>
</tr>
<tr>
<td>5. Specify the mode in which the security protocol encapsulates IP packets.</td>
<td>encapsulation-mode { transport</td>
<td>tunnel }</td>
</tr>
<tr>
<td>6. (Optional.) Enable the Perfect Forward Secrecy (PFS) feature for the IPsec policy.</td>
<td>pfs { dh-group1</td>
<td>dh-group2</td>
</tr>
<tr>
<td>7. (Optional.) Enable the Extended Sequence Number (ESN) feature.</td>
<td>esn enable [ both ]</td>
<td>By default, the ESN feature is disabled.</td>
</tr>
</tbody>
</table>

**Configuring a manual IPsec policy**

In a manual IPsec policy, the parameters are configured manually, such as the keys, the SPIs, and the IP addresses of the two ends in tunnel mode.

**Configuration restrictions and guidelines**

Make sure the IPsec configuration at the two ends of an IPsec tunnel meets the following requirements:
The IPsec policies at the two ends must have IPsec transform sets that use the same security protocols, security algorithms, and encapsulation mode.

The remote IPv4 address configured on the local end must be the same as the primary IPv4 address of the interface applied with the IPsec policy at the remote end. The remote IPv6 address configured on the local end must be the same as the first IPv6 address of the interface applied with the IPsec policy at the remote end.

At each end, configure parameters for both the inbound SA and the outbound SA, and make sure the SAs in each direction are unique: For an outbound SA, make sure its triplet (remote IP address, security protocol, and SPI) is unique. For an inbound SA, make sure its SPI is unique.

The local inbound SA must use the same SPI and keys as the remote outbound SA. The same is true of the local outbound SA and remote inbound SA.

The keys for the local and remote inbound and outbound SAs must be in the same format. For example, if the local inbound SA uses a key in characters, the local outbound SA and remote inbound and outbound SAs must use keys in characters.

**Configuration procedure**

To configure a manual IPsec policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a manual IPsec policy entry and enter its view.</td>
<td>ipsec { ipv6-policy</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Configure a description for the IPsec policy.</td>
<td>description text</td>
</tr>
<tr>
<td>4.</td>
<td>Specify an ACL for the IPsec policy.</td>
<td>security acl [ ipv6 ] { acl-number</td>
</tr>
<tr>
<td>5.</td>
<td>Specify an IPsec transform set for the IPsec policy.</td>
<td>transform-set transform-set-name</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the remote IP address of the IPsec tunnel.</td>
<td>remote-address { ipv4-address</td>
</tr>
</tbody>
</table>
| 7.   | Configure an SPI for the inbound or outbound IPsec SA. | • To configure an SPI for the inbound IPsec SA: sa spi inbound \{ ah | esp \} spi-number  
• To configure an SPI for the outbound IPsec SA: sa spi outbound \{ ah | esp \} spi-number | By default, no SPI is configured for the inbound or outbound IPsec SA. |
### Configuring an IKE-based IPsec policy

In an IKE-based IPsec policy, the parameters are automatically negotiated through IKE.

To configure an IKE-based IPsec policy, use one of the following methods:

- Directly configure it by configuring the parameters in IPsec policy view.
- Configure it by using an existing IPsec policy template with the parameters to be negotiated configured.

A device using an IPsec policy that is configured in this way cannot initiate an SA negotiation, but it can respond to a negotiation request. The parameters not defined in the template are determined by the initiator. When the remote end’s information (such as the IP address) is unknown, this method allows the remote end to initiate negotiations with the local end.

### Configuration restrictions and guidelines

Make sure the IPsec configuration at the two ends of an IPsec tunnel meets the following requirements:

- The IPsec policies at the two tunnel ends must have IPsec transform sets that use the same security protocols, security algorithms, and encapsulation mode.
- The IPsec policies at the two tunnel ends must have the same IKE profile parameters.
- You can specify a maximum of six IPsec transform sets for an IKE-based IPsec policy. During an IKE negotiation, IKE searches for a fully matched IPsec transform set at the two ends of the IPsec tunnel. If no match is found, no SA can be set up, and the packets expecting to be protected will be dropped.
The remote IP address of the IPsec tunnel is required on an IKE negotiation initiator and is optional on the responder. The remote IP address specified on the local end must be the same as the local IP address specified on the remote end.

For an IPsec SA established through IKE negotiation:

- The IPsec SA uses the local lifetime settings or those proposed by the peer, whichever are smaller.
- The IPsec SA can have both a time-based lifetime and a traffic-based lifetime. The IPsec SA expires when either lifetime expires.

Directly configuring an IKE-based IPsec policy

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IKE-based IPsec policy entry and enter its view.</td>
<td>`ipsec { ipv6-policy</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Configure a description for the IPsec policy.</td>
<td><code>description text</code></td>
</tr>
<tr>
<td>4.</td>
<td>Specify an ACL for the IPsec policy.</td>
<td>`security acl [ ipv6 ] { acl-number</td>
</tr>
<tr>
<td>5.</td>
<td>Specify IPsec transform sets for the IPsec policy.</td>
<td><code>transform-set transform-set-name&amp;&lt;1-6&gt;</code></td>
</tr>
<tr>
<td>6.</td>
<td>Specify an IKE profile for the IPsec policy.</td>
<td><code>ike-profile profile-name</code></td>
</tr>
<tr>
<td>7.</td>
<td>Specify an IKEv2 profile for the IPsec policy.</td>
<td><code>ikev2-profile profile-name</code></td>
</tr>
<tr>
<td>8.</td>
<td>Specify the local IP address of the IPsec tunnel.</td>
<td>`local-address { ipv4-address</td>
</tr>
</tbody>
</table>
### Configuring an IKE-based IPsec policy by using an IPsec policy template

The configurable parameters for an IPsec policy template are the same as those when you directly configure an IKE-based IPsec policy. The difference is that more parameters are optional for an IPsec policy template. Except the IPsec transform sets and the IKE profile, all other parameters are optional.

A device using an IPsec policy that is configured by using an IPsec policy template cannot initiate an SA negotiation, but it can respond to a negotiation request. The parameters not defined in the template are determined by the initiator. For example, in an IPsec policy template, the ACL is optional. If you do not specify an ACL, the IPsec protection range has no limit. So the device accepts all ACL settings of the negotiation initiator. When the remote end's information (such as the IP address) is unknown, the IPsec policy configured by using this method allows the remote end to initiate negotiations with the local end.

To configure an IKE-based IPsec policy by using an IPsec policy template:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ipsec { ipv6-policy-template</td>
<td>policy-template } template-name seq-number</td>
</tr>
<tr>
<td>3.</td>
<td>description text</td>
<td>By default, no description is configured.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>4. (Optional.) Specify an ACL for the IPsec policy template.</td>
<td>`security acl [ipv6] { acl-number</td>
<td>name acl-name } [ per-host ]`</td>
</tr>
<tr>
<td>5. Specify IPsec transform sets for the IPsec policy template.</td>
<td><code>transform-set transform-set-name&amp;&lt;1-6&gt;</code></td>
<td>By default, no IPsec transform sets are specified for an IPsec policy template.</td>
</tr>
<tr>
<td>6. Specify an IKE profile for the IPsec policy template.</td>
<td><code>ike-profile profile-name</code></td>
<td>The <code>ikev2-profile</code> command is available in Release 1121 and later. By default, no IKEv2 profile is specified for an IPsec policy template. You can specify only one IKEv2 profile for an IPsec policy template. For more information about IKEv2 profiles, see &quot;Configuring IKEv2.&quot;</td>
</tr>
<tr>
<td>7. Specify an IKEv2 profile for the IPsec policy template.</td>
<td><code>ikev2-profile profile-name</code></td>
<td>By default, no IKE profile is specified for an IPsec policy template. You can specify only one IKE profile for an IPsec policy template. The IKE profile cannot be used by another IPsec policy template or IPsec policy. For more information about IKE profiles, see &quot;Configuring IKE.&quot;</td>
</tr>
<tr>
<td>8. (Optional.) Specify the local IP address of the IPsec tunnel.</td>
<td>`local-address { ipv4-address</td>
<td>ipv6 ipv6-address }`</td>
</tr>
<tr>
<td>9. (Optional.) Specify the remote IP address of the IPsec tunnel.</td>
<td>`remote-address { [ ipv6 ] host-name</td>
<td>ipv4-address</td>
</tr>
<tr>
<td>10. Configure the IPsec SA lifetime.</td>
<td>`sa duration { time-based seconds</td>
<td>traffic-based kilobytes }`</td>
</tr>
<tr>
<td>11. (Optional.) Set the IPsec SA idle timeout.</td>
<td><code>sa idle-time seconds</code></td>
<td>By default, the global SA idle timeout is used.</td>
</tr>
<tr>
<td>12. (Optional.) Enable the Traffic Flow Confidentiality (TFC) padding feature.</td>
<td><code>tfc enable</code></td>
<td>The <code>tfc enable</code> command is available in Release 1121 and later. By default, the TFC padding feature is disabled.</td>
</tr>
</tbody>
</table>
### Applying an IPsec policy to an interface

You can apply an IPsec policy to an interface to protect certain data flows. To cancel the IPsec protection, remove the application of the IPsec policy. In addition to VLAN interfaces, you can apply an IPsec policy to tunnel interfaces to protect applications such as GRE.

For each packet to be sent out of an interface applied with an IPsec policy, the interface looks through the IPsec policy entries in the IPsec policy in ascending order of sequence numbers. If the packet matches the ACL of an IPsec policy entry, the interface uses the IPsec policy entry to protect the packet. If no match is found, the interface sends the packet out without IPsec protection.

When the interface receives an IPsec packet whose destination address is the IP address of the local device, it searches for the inbound IPsec SA according to the SPI carried in the IPsec packet header for de-encapsulation. If the de-encapsulated packet matches the permit rule of the ACL, the device processes the packet. Otherwise, it drops the packet.

An interface can have only one IPsec policy applied. An IKE-based IPsec policy can be applied to more than one interface, but a manual IPsec policy can be applied to only one interface.

To apply an IPsec policy to an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Apply an IPsec policy to the interface.</td>
<td>By default, no IPsec policy is applied to the interface.</td>
</tr>
<tr>
<td></td>
<td>ipsec apply { policy</td>
<td>ipv6-policy } policy-name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An IKE-mode IPsec policy can be applied to multiple interfaces, and a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>manual IPsec policy can be applied to only one interface.</td>
</tr>
</tbody>
</table>

### Enabling ACL checking for de-encapsulated packets

This feature uses the ACL in the IPsec policy to match the IP packets that are de-encapsulated from incoming IPsec packets in tunnel mode, and it discards the IP packets that fail to match the ACL to avoid attacks using forged packets.
To enable ACL checking for de-encapsulated packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable ACL checking for de-encapsulated packets.</td>
<td>ipsec decrypt-check enable</td>
</tr>
</tbody>
</table>

### Configuring IPsec anti-replay

The IPsec anti-replay feature protects networks against anti-replay attacks by using a sliding window mechanism called anti-replay window. This feature checks the sequence number of each received IPsec packet against the current IPsec packet sequence number range of the sliding window. If the sequence number is not in the current sequence number range, the packet is considered a replayed packet and is discarded.

IPsec packet de-encapsulation involves complicated calculation. De-encapsulation of replayed packets is not required, and the de-encapsulation process consumes large amounts of resources and degrades performance, resulting in DoS. IPsec anti-replay can check and discard replayed packets before de-encapsulation.

In some situations, service data packets are received in a different order than their original order. The IPsec anti-replay feature drops them as replayed packets, which impacts communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

IPsec anti-replay does not affect manually created IPsec SAs. According to the IPsec protocol, only IKE-based IPsec SAs support anti-replay checking.

**IMPORTANT:**
- IPsec anti-replay is enabled by default. Failure to detect anti-replay attacks might result in denial of services. Use caution when you disable IPsec anti-replay.
- Specify an anti-replay window size that is as small as possible to reduce the impact on system performance.
- IPsec anti-replay requires that packets on the same interface be processed on the same slot. To perform IPsec anti-replay on a multichassis IRF fabric for a VLAN or tunnel interface, use the service command in interface view to specify a service processing slot for that interface. For more information about the service command, see Layer 2—LAN Switching Command Reference.

To configure IPsec anti-replay:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable IPsec anti-replay.</td>
<td>ipsec anti-replay check</td>
</tr>
<tr>
<td>3.</td>
<td>Set the size of the IPsec anti-replay window.</td>
<td>ipsec anti-replay window width</td>
</tr>
</tbody>
</table>

### Configuring IPsec anti-replay redundancy

This feature synchronizes the following information from the master device to all subordinate devices in an IRF fabric at configurable packet-based intervals:
- Lower bound values of the IPsec anti-replay window for inbound packets.
IPsec anti-replay sequence numbers for outbound packets.

This feature, used together with IPsec redundancy, ensures uninterrupted IPsec traffic forwarding and anti-replay protection when the master device in an IRF fabric fails.

To configure IPsec anti-replay redundancy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable IPsec redundancy.</td>
<td>ipsec redundancy enable</td>
</tr>
</tbody>
</table>
| 3.   | Enter IPsec policy view or IPsec policy template view. | - Enter IPsec policy view:
  `ipsec { policy | ipv6-policy }
policy-name seq-number
  [ isakmp | manual ]`

  - Enter IPsec policy template view:
  `ipsec { policy-template | ipv6-policy-template }
template-name seq-number`
| 4.   | Set the anti-replay window synchronization interval for inbound packets and the sequence number synchronization interval for outbound packets. | redundancy replay-interval inbound inbound-interval outbound outbound-interval | By default, the master device synchronizes the anti-replay window every time it receives 1000 packets and the sequence number every time it sends 100000 packets. |

**Binding a source interface to an IPsec policy**

For high availability, a core device is usually connected to an ISP through two links, which operate in backup or load sharing mode. The two interfaces negotiate with their peers to establish IPsec SAs respectively. When one interface fails and a link failover occurs, the other interface needs to take some time to renegotiate SAs, resulting in service interruption.

To solve these problems, bind a source interface to an IPsec policy and apply the policy to both interfaces. This enables the two physical interfaces to use the same source interface to negotiate IPsec SAs. As long as the source interface is up, the negotiated IPsec SAs will not be removed and will keep working, regardless of link failover.

Follow these guidelines when you perform this task:

- Only the IKE-based IPsec policies can be bound to a source interface.
- An IPsec policy can be bound to only one source interface.
- A source interface can be bound to multiple IPsec policies.
- If the source interface bound to an IPsec policy is removed, the IPsec policy becomes a common IPsec policy.
- If no local address is specified for an IPsec policy that has been bound to a source interface, the IPsec policy uses the IP address of the bound source interface to perform IKE negotiation. If a local address is specified, the IPsec policy uses the local address to perform IKE negotiation.

To bind a source interface to an IPsec policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Bind a source interface to an IPsec policy. | ipsec { ipv6-policy | policy }
policy-name local-address | By default, no source interface is bound to an IPsec policy. |
Enabling QoS pre-classify

If you apply both an IPsec policy and a QoS policy to an interface, QoS classifies packets by using the new headers added by IPsec. If you want QoS to classify packets by using the headers of the original IP packets, enable the QoS pre-classify feature.

For more information about QoS policy and classification, see ACL and QoS Configuration Guide.

To enable the QoS pre-classify feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter IPsec policy view or IPsec policy template view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Enable QoS pre-classify.</td>
<td>qos pre-classify</td>
</tr>
</tbody>
</table>

Enabling logging of IPsec packets

Perform this task to enable the logging of IPsec packets that are discarded because of reasons such as IPsec SA lookup failure, AH-ESP authentication failure, and ESP encryption failure. The log information includes the source and destination IP addresses, the SPI value, and the sequence number of a discarded IPsec packet, and the reason for the failure.

To enable the logging of IPsec packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the logging of IPsec packets.</td>
<td>ipsec logging packet enable</td>
</tr>
</tbody>
</table>

Configuring the DF bit of IPsec packets

Perform this task to configure the Don't Fragment (DF) bit in the new IP header of IPsec packets in one of the following ways:

- **clear**—Clears the DF bit in the new header.
- **set**—Sets the DF bit in the new header.
- **copy**—Copies the DF bit in the original IP header to the new IP header.
You can configure the DF bit in system view and interface view. The interface-view DF bit setting takes precedence over the system-view DF bit setting. If the interface-view DF bit setting is not configured, the interface uses the system-view DF bit setting.

Follow these guidelines when you configure the DF bit:

- The DF bit setting takes effect only in tunnel mode, and it changes the DF bit in the new IP header rather than the original IP header.
- Configure the same DF bit setting on the interfaces where the same IPsec policy bound to a source interface has been applied.

To configure the DF bit of IPsec packets on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>interface-type</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the DF bit of IPsec</td>
<td>ipsec df-bit { clear</td>
</tr>
<tr>
<td></td>
<td>packets on the interface.</td>
<td>By default, the interface uses the global DF bit setting.</td>
</tr>
</tbody>
</table>

To configure the DF bit of IPsec packets globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the DF bit of IPsec</td>
<td>ipsec global-df-bit { clear</td>
</tr>
<tr>
<td></td>
<td>packets globally.</td>
<td>By default, IPsec copies the DF bit in the original IP header to the new IP header.</td>
</tr>
</tbody>
</table>

### Configuring IPsec for IPv6 routing protocols

#### Configuration task list

Complete the following tasks to configure IPsec for IPv6 routing protocols:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>*(Required.) Configuring an IPsec transform set</td>
</tr>
<tr>
<td>*(Required.) Configuring a manual IPsec profile</td>
</tr>
<tr>
<td>*(Required.) Applying the IPsec profile to an IPv6 routing protocol (see Layer 3—IP Routing Configuration Guide)</td>
</tr>
<tr>
<td>*(Optional.) Enabling logging of IPsec packets</td>
</tr>
<tr>
<td>*(Optional.) Configuring SNMP notifications for IPsec</td>
</tr>
</tbody>
</table>
Configuring a manual IPsec profile

An IPsec profile is similar to an IPsec policy. The difference is that an IPsec profile is uniquely identified by a name and it does not support ACL configuration. An IPsec profile defines the IPsec transform set used for protecting data flows, and specifies SPIs and the keys used by the SAs.

The IPsec profile configurations at the two tunnel ends must meet the following requirements:

- The IPsec transform set used by the IPsec profile at the two tunnel ends must have the same security protocol, encryption and authentication algorithms, and packet encapsulation mode.
- The local inbound and outbound IPsec SAs must have the same SPI and key.
  - The IPsec SAs on the devices in the same scope must have the same key. The scope is defined by protocols. For RIPng, the scope consists of directly-connected neighbors or a RIPng process. For OSPF, the scope consists of OSPF neighbors or an OSPF area. For BGP, the scope consists of BGP peers or a BGP peer group.
- The keys for the IPsec SAs at the two tunnel ends must be configured in the same format. For example, if the key at one end is entered as a string of characters, the key on the other end must also be entered as a string of characters.

To configure a manual IPsec profile:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a manual IPsec profile and enter its view.</td>
<td>ipsec profile profile-name manual</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Configure a description for the IPsec profile.</td>
<td>description text</td>
</tr>
<tr>
<td>4.</td>
<td>Specify an IPsec transform set for the IPsec profile.</td>
<td>transform-set transform-set-name</td>
</tr>
<tr>
<td>5.</td>
<td>Configure an SPI for an SA.</td>
<td>sa { inbound</td>
</tr>
</tbody>
</table>
### Configuring SNMP notifications for IPsec

After you enable SNMP notifications for IPsec, the IPsec module notifies the NMS of important module events. The notifications are sent to the device’s SNMP module. You can configure the notification transmission parameters for the SNMP module to specify how the SNMP module displays notifications. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

To generate and output SNMP notifications for a specific IPsec failure or event type, perform the following tasks:

1. Enable SNMP notifications for IPsec globally.
2. Enable SNMP notifications for the failure or event type.

To configure SNMP notifications for IPsec:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable SNMP notifications for IPsec globally.</td>
<td>snmp-agent trap enable ipsec global</td>
</tr>
<tr>
<td>3.</td>
<td>Enable SNMP notifications for the specified failure or event types.</td>
<td>snmp-agent trap enable ipsec [ auth-failure</td>
</tr>
</tbody>
</table>
Displaying and maintaining IPsec

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display IPsec policy information.</td>
<td>`display ipsec { ipv6-policy</td>
</tr>
<tr>
<td>Display IPsec policy template information.</td>
<td>`display ipsec { ipv6-policy-template</td>
</tr>
<tr>
<td>Display IPsec profile information.</td>
<td><code>display ipsec profile [ profile-name ]</code></td>
</tr>
<tr>
<td>Display IPsec transform set information.</td>
<td><code>display ipsec transform-set [ transform-set-name ]</code></td>
</tr>
<tr>
<td>Display IPsec SA information.</td>
<td>`display ipsec sa [ brief</td>
</tr>
<tr>
<td>Display IPsec statistics.</td>
<td><code>display ipsec statistics [ tunnel-id tunnel-id ]</code></td>
</tr>
<tr>
<td>Display IPsec tunnel information.</td>
<td>`display ipsec tunnel { brief</td>
</tr>
<tr>
<td>Clear IPsec SAs.</td>
<td>`reset ipsec sa [ { ipv6-policy</td>
</tr>
<tr>
<td>Clear IPsec statistics.</td>
<td><code>reset ipsec statistics [ tunnel-id tunnel-id ]</code></td>
</tr>
</tbody>
</table>

IPsec configuration examples

Configuring a manual mode IPsec tunnel for IPv4 packets

Network requirements

As shown in Figure 86, establish an IPsec tunnel between Switch A and Switch B to protect data flows between the switches. Configure the tunnel as follows:

- Specify the encapsulation mode as tunnel, the security protocol as ESP, the encryption algorithm as AES-CBC-192, and the authentication algorithm as HMAC-SHA1.
- Manually set up IPsec SAs.

Figure 86 Network diagram

![Network diagram](image)

Configuration procedure

1. Configure Switch A:
   ```
   # Configure an IP address for VLAN-interface 1.
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 1
   ```
# Configure an ACL to identify data flows between Switch A and Switch B.
[SwitchA] acl number 3101
[SwitchA-acl-adv-3101] rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
[SwitchA-acl-adv-3101] quit

# Create an IPsec transform set named tran1.
[SwitchA] ipsec transform-set tran1

# Specify the encapsulation mode as tunnel.
[SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel

# Specify the security protocol as ESP.
[SwitchA-ipsec-transform-set-tran1] protocol esp

# Specify the ESP encryption and authentication algorithms.
[SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-transform-set-tran1] quit

# Create a manual IPsec policy entry. Specify the policy name as map1 and set the sequence number to 10.
[SwitchA] ipsec policy map1 10 manual

# Apply ACL 3101.
[SwitchA-ipsec-policy-manual-map1-10] security acl 3101

# Apply the IPsec transform set tran1.
[SwitchA-ipsec-policy-manual-map1-10] transform-set tran1

# Specify the remote IP address of the IPsec tunnel as 2.2.3.1.
[SwitchA-ipsec-policy-manual-map1-10] remote-address 2.2.3.1

# Configure inbound and outbound SPIs for ESP.
[SwitchA-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[SwitchA-ipsec-policy-manual-map1-10] sa spi inbound esp 54321

# Configure the inbound and outbound SA keys for ESP.
[SwitchA-ipsec-policy-manual-map1-10] sa string-key outbound esp simple abcdefg
[SwitchA-ipsec-policy-manual-map1-10] sa string-key inbound esp simple gfedcba
[SwitchA-ipsec-policy-manual-map1-10] quit

# Apply the IPsec policy map1 to interface VLAN-interface 1.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec apply policy map1

2. Configure Switch B:

# Configure an IP address for VLAN-interface 1.
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
[SwitchB-Vlan-interface1] quit

# Configure an ACL to identify data flows between Switch B and Switch A.
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchB-acl-adv-3101] quit

# Create an IPsec transform set named tran1.
[SwitchB] ipsec transform-set tran1
# Specify the encapsulation mode as tunnel.
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel

# Specify the security protocol as ESP.
[SwitchB-ipsec-transform-set-tran1] protocol esp

# Specify the ESP encryption and authentication algorithms.
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-tran1] quit

# Create a manual IPsec policy entry. Specify the policy name as use1 and set the sequence number to 10.
[SwitchB] ipsec policy use1 10 manual

# Apply ACL 3101.
[SwitchB-ipsec-policy-manual-use1-10] security acl 3101

# Apply IPsec transform set tran1.
[SwitchB-ipsec-policy-manual-use1-10] transform-set tran1

# Specify the remote IP address of the IPsec tunnel as 2.2.2.1.
[SwitchB-ipsec-policy-manual-use1-10] remote-address 2.2.2.1

# Configure the inbound and outbound SPIs for ESP.
[SwitchB-ipsec-policy-manual-use1-10] sa spi outbound esp 54321
[SwitchB-ipsec-policy-manual-use1-10] sa spi inbound esp 12345

# Configure the inbound and outbound SA keys for ESP.
[SwitchB-ipsec-policy-manual-use1-10] sa string-key outbound esp simple gfedcba
[SwitchB-ipsec-policy-manual-use1-10] sa string-key inbound esp simple abcdefg
[SwitchB-ipsec-policy-manual-use1-10] quit

# Apply the IPsec policy use1 to interface VLAN-interface 1.
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec apply policy use1

Verifying the configuration

After the configuration is completed, an IPsec tunnel between Switch A and Switch B is established, and the traffic between the switches is IPsec protected. This example uses Switch A to verify the configuration.

# Use the display ipsec sa command to display IPsec SAs on Switch A.
[SwitchA] display ipsec sa

-------------------------------
Interface: Vlan-interface 1
-------------------------------

-------------------------------
IPsec policy: map1
Sequence number: 10
Mode: manual
-------------------------------
Tunnel id: 549
Encapsulation mode: tunnel
Path MTU: 1443
Tunnel:
  local address: 2.2.2.1
remote address: 2.2.3.1
Flow:
as defined in ACL 3101
[Inbound ESP SA]
SPI: 54321 (0x0000d431)
Transform set: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
No duration limit for this SA
[Outbound ESP SA]
SPI: 12345 (0x00003039)
Transform set: ESP-ENCRYPT-AES-CBC-192 ESP-AUTH-SHA1
No duration limit for this SA

Configuring an IKE-based IPsec tunnel for IPv4 packets

Network requirements

As shown in Figure 87, establish an IPsec tunnel between Switch A and Switch B to protect data flows between the switches. Configure the IPsec tunnel as follows:

- Specify the encapsulation mode as tunnel, the security protocol as ESP, the encryption algorithm as AES-CBC-192, and the authentication algorithm as HMAC-SHA1.
- Set up SAs through IKE negotiation.

Figure 87 Network diagram

- Internet
- Vlan-int1 2.2.2.1/24
- Switch A
- Vlan-int1 2.2.3.1/24
- Switch B

Configuration procedure

1. Configure Switch A:
   # Configure an IP address for VLAN-interface 1.
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 1
   [SwitchA-Vlan-interface1] ip address 2.2.2.1 255.255.255.0
   [SwitchA-Vlan-interface1] quit
   # Configure an ACL to identify data flows between Switch A and Switch B.
   [SwitchA] acl number 3101
   [SwitchA-acl-adv-3101] rule 0 permit ip source 2.2.2.1 0 destination 2.2.3.1 0
   [SwitchA-acl-adv-3101] quit
   # Create an IPsec transform set named tran1.
   [SwitchA] ipsec transform-set tran1
   # Specify the encapsulation mode as tunnel.
   [SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel
   # Specify the security protocol as ESP.
   [SwitchA-ipsec-transform-set-tran1] protocol esp
   # Specify the ESP encryption and authentication algorithms.
   [SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
   [SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchA-ipsec-transform-set-tran1] quit
# Create the IKE keychain named keychain1.
[SwitchA] ike keychain keychain1

# Specify 12345zxcvb!@#$%ZXCVB in plain text as the pre-shared key to be used with the peer 2.2.3.1.
[SwitchA-ike-keychain-keychain1] pre-shared-key address 2.2.3.1 255.255.255.0 key simple 12345zxcvb!@#$%ZXCVB
[SwitchA-ike-keychain-keychain1] quit

# Create the IKE profile named profile1.
[SwitchA] ike profile profile1

# Specify the keychain keychain1.
[SwitchA-ike-profile-profile1] keychain keychain1
[SwitchA-ike-profile-profile1] match remote identity address 2.2.3.1 255.255.255.0
[SwitchA-ike-profile-profile1] quit

# Create an IKE-based IPsec policy entry. Specify the policy name as map1 and set the sequence number to 10.
[SwitchA] ipsec policy map1 10 isakmp

# Apply ACL 3101.
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101

# Apply the IPsec transform set tran1.
[SwitchA-ipsec-policy-isakmp-map1-10] transform-set tran1

# Specify the local and remote IP addresses of the IPsec tunnel as 2.2.2.1 and 2.2.3.1.
[SwitchA-ipsec-policy-isakmp-map1-10] local-address 2.2.2.1
[SwitchA-ipsec-policy-isakmp-map1-10] remote-address 2.2.3.1

# Apply the IKE profile profile1.
[SwitchA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[SwitchA-ipsec-policy-isakmp-map1-10] quit

# Specify slot 1 as the traffic processing slot for VLAN-interface 1.
[SwitchA-Vlan-interface1] service slot 1

# Apply the IPsec policy map1 to VLAN-interface 1.
[SwitchA-Vlan-interface1] ipsec apply policy map1

2. Configure Switch B:

# Configure an IP address for VLAN-interface 1.
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 2.2.3.1 255.255.255.0
[SwitchB-Vlan-interface1] quit

# Configure an ACL to identify data flows between Switch B and Switch A.
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.3.1 0 destination 2.2.2.1 0
[SwitchB-acl-adv-3101] quit

# Create an IPsec transform set named tran1.
[SwitchB] ipsec transform-set tran1

# Specify the encapsulation mode as tunnel.
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel

# Specify the security protocol as ESP.
[SwitchB-ipsec-transform-set-tran1] protocol esp
# Specify the ESP encryption and authentication algorithms.
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-tran1] quit

# Create the IKE keychain named keychain1.
[SwitchB] ike keychain keychain1

# Specify 12345zxcvb@#$%ZXCVB in plain text as the pre-shared key to be used with the peer 2.2.2.1.
[SwitchB-ike-keychain-keychain1] pre-shared-key address 2.2.2.1 255.255.255.0 key simple 12345zxcvb@#$%ZXCVB
[SwitchB-ike-keychain-keychain1] quit

# Create the IKE profile named profile1.
[SwitchB] ike profile profile1

# Specify the keychain keychain1.
[SwitchB-ike-profile-profile1] keychain keychain1
[SwitchB-ike-profile-profile1] match remote identity address 2.2.2.1 255.255.255.0
[SwitchB-ike-profile-profile1] quit

# Create an IKE-based IPsec policy entry. Specify the policy name as use1 and set the sequence number to 10.
[SwitchB] ipsec policy use1 10 isakmp

# Apply ACL 3101.
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101

# Apply the IPsec transform set tran1.
[SwitchB-ipsec-policy-isakmp-use1-10] transform-set tran1

# Specify the local and remote IP addresses of the IPsec tunnel as 2.2.3.1 and 2.2.2.1.
[SwitchB-ipsec-policy-isakmp-map1-10] local-address 2.2.3.1
[SwitchB-ipsec-policy-isakmp-use1-10] remote-address 2.2.2.1

# Apply the IKE profile profile1.
[SwitchB-ipsec-policy-isakmp-use1-10] ike-profile profile1
[SwitchB-ipsec-policy-isakmp-use1-10] quit

# Specify slot 1 as the traffic processing slot for VLAN-interface 1.
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] service slot 1

# Apply the IPsec policy use1 to interface VLAN-interface 1.
[SwitchB-Vlan-interface1] ipsec apply policy use1

Verifying the configuration
# Initiate a connection from Switch A to Switch B to trigger the IKE negotiation. After IPsec SAs are successfully negotiated by IKE, the traffic between the two switches is IPsec protected.

Configuring IPsec for RIPng

Network requirements
As shown in Figure 88, Switch A, Switch B, and Switch C learn IPv6 routes through RIPng.
Establish an IPsec tunnel between the switches to protect the RIPng packets transmitted in between. Specify the security protocol as ESP, the encryption algorithm as 128-bit AES, and the authentication algorithm as HMAC-SHA1 for the IPsec tunnel.
Requirements analysis

To meet the network requirements, perform the following tasks:

1. Configure basic RIPng.
   
   For more information about RIPng configurations, see *Layer 3—IP Routing Configuration Guide*.

2. Configure an IPsec profile.
   
   - The IPsec profiles on all the switches must have IPsec transform sets that use the same security protocol, authentication and encryption algorithms, and encapsulation mode.
   
   - The SPI and key configured for the inbound SA and those for the outbound SA must be the same on each switch.

   - The SPI and key configured for the SAs on all the switches must be the same.

3. Apply the IPsec profile to a RIPng process or to an interface.

Configuration procedure

1. Configure Switch A:

   # Configure IPv6 addresses for interfaces. (Details not shown.)
   
   # Configure basic RIPng.

   ```
   <SwitchA> system-view
   [SwitchA] ripng 1
   [SwitchA-ripng-1] quit
   [SwitchA] interface vlan-interface 100
   [SwitchA-Vlan-interface100] ripng 1 enable
   [SwitchA-Vlan-interface100] quit
   ```

   # Create and configure the IPsec transform set named tran1.

   ```
   [SwitchA] ipsec transform-set tran1
   [SwitchA-ipsec-transform-set-tran1] encapsulation-mode transport
   [SwitchA-ipsec-transform-set-tran1] protocol esp
   [SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
   [SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchA-ipsec-transform-set-tran1] quit
   ```

   # Create and configure the IPsec profile named profile001.

   ```
   [SwitchA] ipsec profile profile001 manual
   [SwitchA-ipsec-profile-profile1001] transform-set tran1
   [SwitchA-ipsec-profile-profile1001] sa spi outbound esp 123456
   [SwitchA-ipsec-profile-profile1001] sa spi inbound esp 123456
   [SwitchA-ipsec-profile-profile1001] sa string-key outbound esp simple abcdefg
   [SwitchA-ipsec-profile-profile1001] sa string-key inbound esp simple abcdefg
   [SwitchA-ipsec-profile-profile1001] quit
   ```

   # Apply the IPsec profile to RIPng process 1.

   ```
   [SwitchA] ripng 1
   [SwitchA-ripng-1] enable ipsec-profile profile001
   [SwitchA-ripng-1] quit
   ```
2. Configure Switch B:
   # Configure IPv6 addresses for interfaces. (Details not shown.)
   # Configure basic RIPng.
   <SwitchB> system-view
   [SwitchB] ripng 1
   [SwitchB-ripng-1] quit
   [SwitchB] interface vlan-interface 200
   [SwitchB-Vlan-interface200] ripng 1 enable
   [SwitchB-Vlan-interface200] quit
   [SwitchB] interface vlan-interface 100
   [SwitchB-Vlan-interface100] ripng 1 enable
   [SwitchB-Vlan-interface100] quit
   # Create and configure the IPsec transform set named tran1.
   [SwitchB] ipsec transform-set tran1
   [SwitchB-ipsec-transform-set-tran1] encapsulation-mode transport
   [SwitchB-ipsec-transform-set-tran1] protocol esp
   [SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
   [SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchB-ipsec-transform-set-tran1] quit
   # Create and configure the IPsec profile named profile001.
   [SwitchB] ipsec profile profile001 manual
   [SwitchB-ipsec-profile-profile001] transform-set tran1
   [SwitchB-ipsec-profile-profile001] sa spi outbound esp 123456
   [SwitchB-ipsec-profile-profile001] sa spi inbound esp 123456
   [SwitchB-ipsec-profile-profile001] sa string-key outbound esp simple abcd
   [SwitchB-ipsec-profile-profile001] sa string-key inbound esp simple abcd
   [SwitchB-ipsec-profile-profile001] quit
   # Apply the IPsec profile to RIPng process 1.
   [SwitchB] ripng 1
   [SwitchB-ripng-1] enable ipsec-profile profile001
   [SwitchB-ripng-1] quit

3. Configure Switch C:
   # Configure IPv6 addresses for interfaces. (Details not shown.)
   # Configure basic RIPng.
   <SwitchC> system-view
   [SwitchC] ripng 1
   [SwitchC-ripng-1] quit
   [SwitchC] interface vlan-interface 200
   [SwitchC-Vlan-interface200] ripng 1 enable
   [SwitchC-Vlan-interface200] quit
   # Create and configure the IPsec transform set named tran1.
   [SwitchC] ipsec transform-set tran1
   [SwitchC-ipsec-transform-set-tran1] encapsulation-mode transport
   [SwitchC-ipsec-transform-set-tran1] protocol esp
   [SwitchC-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
   [SwitchC-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchC-ipsec-transform-set-tran1] quit
# Create and configure the IPsec profile named profile001.

```plaintext
[SwitchC] ipsec profile profile001 manual
[SwitchC-ipsec-profile-profile001] transform-set tran1
[SwitchC-ipsec-profile-profile001] sa spi outbound esp 123456
[SwitchC-ipsec-profile-profile001] sa spi inbound esp 123456
[SwitchC-ipsec-profile-profile001] sa string-key outbound esp simple abcedfg
[SwitchC-ipsec-profile-profile001] sa string-key inbound esp simple abcedfg
[SwitchC-ipsec-profile-profile001] quit
```

# Apply the IPsec profile to RIPng process 1.

```plaintext
[SwitchC] ripng 1
[SwitchC-ripng-1] enable ipsec-profile profile001
[SwitchC-ripng-1] quit
```

## Verifying the configuration

After the configuration is completed, Switch A, Switch B, and Switch C learn IPv6 routing information through RIPng. IPsec SAs are set up successfully on the switches to protect RIPng packets. This example uses Switch A to verify the configuration.

# Use the `display ripng` command to display the RIPng configuration. The output shows that the IPsec profile `profile001` has been applied to RIPng process 1.

```plaintext
[SwitchA] display ripng 1
RIPng process : 1
 Preference : 100
 Checkzero : Enabled
 Default Cost : 0
 Maximum number of balanced paths : 8
 Update time   :   30 sec(s) Timeout time         :  180 sec(s)
 Suppress time :  120 sec(s) Garbage-Collect time :  120 sec(s)
 Number of periodic updates sent : 186
 Number of trigger updates sent : 1
IPsec profile name: profile001
```

# Use the `display ipsec sa` command to display the established IPsec SAs.

```plaintext
[SwitchA] display ipsec sa
-------------------------------
Global IPsec SA
-------------------------------
IPsec profile: profile001
 Mode: manual
-------------------------------
Encapsulation mode: transport
[Inbound ESP SA]
 SPI: 123456 (0x3039)
 Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
 No duration limit for this SA
[Outbound ESP SA]
 SPI: 123456 (0x3039)
 Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
```
No duration limit for this SA
Configuring IKE

Unless otherwise specified, the term "IKE" in this chapter refers to IKEv1.
The term "interface" in this chapter collectively refers to Layer 3 interfaces, including VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see Layer 2—LAN Switching Configuration Guide).

Overview

Built on a framework defined by ISAKMP, Internet Key Exchange (IKE) provides automatic key negotiation and SA establishment services for IPsec.

IKE provides the following benefits for IPsec:
- Automatically negotiates IPsec parameters.
- Performs DH exchanges to calculate shared keys, making sure each SA has a key that is independent of other keys.
- Automatically negotiates SAs when the sequence number in the AH or ESP header overflows, making sure IPsec can provide the anti-replay service by using the sequence number.

As shown in Figure 89, IKE negotiates SAs for IPsec and transfers the SAs to IPsec, and IPsec uses the SAs to protect IP packets.

**Figure 89 Relationship between IKE and IPsec**

IKE negotiation process

IKE negotiates keys and SAs for IPsec in two phases:
1. **Phase 1**—The two peers establish an IKE SA, a secure, authenticated channel for communication. In this phase, two modes are available: main mode and aggressive mode.
2. **Phase 2**—Using the IKE SA established in phase 1, the two peers negotiate to establish IPsec SAs.
As shown in Figure 90, the main mode of IKE negotiation in phase 1 involves three pairs of messages:

- **SA exchange**—Used for negotiating the IKE security policy.
- **Key exchange**—Used for exchanging the DH public value and other values, such as the random number. The two peers use the exchanged data to generate key data and use the encryption key and authentication key to ensure the security of IP packets.
- **ID and authentication data exchange**—Used for identity authentication.

The main difference between the main mode and the aggressive mode is that the aggressive mode does not provide identity information protection and exchanges only three messages, rather than three pairs. The main mode provides identity information protection but is slower.

**IKE security mechanism**

IKE has a series of self-protection mechanisms and supports secure identity authentication, key distribution, and IPsec SA establishment on insecure networks.

**Identity authentication**

The IKE identity authentication mechanism is used to authenticate the identity of the communicating peers. The device supports the following identity authentication methods:

- **Pre-shared key authentication**—Two communicating peers use the pre-configured shared key for identity authentication.
- **RSA signature authentication** and **DSA signature authentication**—Two communicating peers use the digital certificates issued by the CA for identity authentication.

The pre-shared key authentication method does not require certificates and is easy to configure. It is usually deployed in small networks.

The signature authentication methods provide higher security and are usually deployed in networks with the headquarters and some branches. When deployed in a network with many branches, a signature authentication method can simplify the configuration because only one PKI domain is required. If you use the pre-shared key authentication method, you must configure a pre-shared key for each branch on the Headquarters node.
DH algorithm

The DH algorithm is a public key algorithm. With this algorithm, two peers can exchange keying material and then use the material to calculate the shared keys. Due to the decryption complexity, a third party cannot decrypt the keys even after intercepting all keying materials.

PFS

The Perfect Forward Secrecy (PFS) feature is a security feature based on the DH algorithm. After PFS is enabled, an additional DH exchange is performed in IKE phase 2 to make sure IPsec keys have no derivative relations with IKE keys and a broken key brings no threats to other keys.

Protocols and standards

- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2412, *The OAKLEY Key Determination Protocol*

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see “Configuring FIPS”) and non-FIPS mode.

IKE configuration prerequisites

Determine the following parameters prior to IKE configuration:

- The algorithms to be used during IKE negotiation, including the identity authentication method, encryption algorithm, authentication algorithm, and DH group.
  - Different algorithms provide different levels of protection. A stronger algorithm provides more resistance to decryption but uses more resources.
  - A DH group that uses more bits provides higher security but needs more time for processing.
- The pre-shared key or PKI domain for IKE negotiation. For more information about PKI, see "Configuring PKI."
- The IKE-based IPsec policies for the communicating peers. If you do not specify an IKE profile for an IPsec policy, the device selects an IKE profile for the IPsec policy. If no IKE profile is configured, the globally configured IKE settings are used. For more information about IPsec, see "Configuring an IKE-based IPsec policy."

IKE configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Configuring an IKE profile</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Configuring an IKE proposal</td>
<td>Required when you specify IKE proposals for the IKE profile.</td>
</tr>
<tr>
<td>(Optional.) Configuring an IKE keychain</td>
<td>Required when pre-shared authentication is used in IKE negotiation phase 1.</td>
</tr>
<tr>
<td>(Optional.) Configuring the global identity information</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Configuring an IKE profile

An IKE profile is intended to provide a set of parameters for IKE negotiation. To configure an IKE profile, you can do the following:

1. **Configure peer IDs.** When an end needs to select an IKE profile, it matches the received peer ID against the peer IDs of its local IKE profiles. If a match is found, it uses the IKE profile with the peer ID for IKE negotiation.

2. **Configure the IKE keychain or PKI domain for the IKE proposals to use:**
   - To use digital signature authentication, configure a PKI domain.
   - To use pre-shared key authentication, configure an IKE keychain.

3. **Specify the negotiation mode (main or aggressive) that the device uses as the initiator.** When the device acts as the responder, it uses the IKE negotiation mode of the initiator.

4. **Specify the IKE proposals that the device can use as the initiator.** An IKE proposal specified earlier has a higher priority. When the device acts as the responder, it uses the IKE proposals configured in system view to match the IKE proposals received from the initiator. If a match is not found, the negotiation fails.

5. **Configure the local ID, the ID that the device uses to identify itself to the peer during IKE negotiation:**
   - For digital signature authentication, the device can use any type of ID. If the local ID is an IP address that is different from the IP address in the local certificate, the device uses the FQDN (the device name configured by using the `sysname` command) instead.
   - For pre-shared key authentication, the device can use any type of ID other than the DN.

6. **Configure the IKE DPD feature to detect dead IKE peers.** You can also configure this feature in system view. The IKE DPD settings configured in the IKE profile takes precedence over those configured in system view.

7. **Specify a local interface or IP address for the IKE profile so the profile can be applied only to the specified interface or IP address.** For this task, specify the local address configured in IPsec policy or IPsec policy template view (using the `local-address` command). If no local address is configured, specify the IP address of the interface to which the IPsec policy is applied.

8. **Specify a priority number for the IKE profile.** To determine the priority of an IKE profile:
   - **First,** the device examines the existence of the `match local address` command. An IKE profile with the `match local address` command configured has a higher priority.
   - **If a tie exists,** the device compares the priority numbers. An IKE profile with a smaller priority number has a higher priority.
   - **If a tie still exists,** the device prefers an IKE profile configured earlier.

To configure an IKE profile:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IKE profile and enter its view.</td>
<td>ike profile profile-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a peer ID.</td>
<td>match remote { certificate policy-name</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the keychain for pre-shared key authentication or the PKI domain used to request a certificate for digital signature authentication.</td>
<td>• To specify the keychain for pre-shared key authentication: keychain keychain-name • To specify the PKI domain used to request a certificate for digital signature authentication: certificate domain domain-name</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the IKE negotiation mode for phase 1.</td>
<td>• In non-FIPS mode: exchange-mode { aggressive</td>
</tr>
<tr>
<td>6.</td>
<td>Specify IKE proposals for the IKE profile.</td>
<td>proposal proposal-number&lt;1-6&gt;</td>
</tr>
<tr>
<td>7.</td>
<td>Configure the local ID.</td>
<td>local-identity { address { ipv4-address</td>
</tr>
<tr>
<td>8.</td>
<td>(Optional.) Configure IKE DPD.</td>
<td>dpd interval interval-seconds [ retry seconds ] { on-demand</td>
</tr>
<tr>
<td>9.</td>
<td>(Optional.) Specify the local interface or IP address to which the IKE profile can be applied.</td>
<td>match local address { interface-type interface-number</td>
</tr>
</tbody>
</table>
### Configuring an IKE proposal

An IKE proposal defines a set of attributes describing how IKE negotiation in phase 1 should take place. You can create multiple IKE proposals with different priorities. The priority of an IKE proposal is represented by its sequence number. The lower the sequence number, the higher the priority.

Two peers must have at least one matching IKE proposal for successful IKE negotiation. During IKE negotiation:

- The initiator sends its IKE proposals to the peer.
  - If the initiator is using an IPsec policy with an IKE profile, the initiator sends all IKE proposals specified for the IKE profile to the peer. An IKE proposal specified earlier for the IKE profile has a higher priority.
  - If the initiator is using an IPsec policy with no IKE profile, the initiator sends all its IKE proposals to the peer. An IKE proposal with a smaller number has a higher priority.

- The peer searches its own IKE proposals for a match. The search starts from the IKE proposal with the highest priority and proceeds in descending order of priority until a match is found. The matching IKE proposals are used to establish the IKE SA. If all user-defined IKE proposals are found mismatching, the two peers use their default IKE proposals to establish the IKE SA.

Two matching IKE proposals have the same encryption algorithm, authentication method, authentication algorithm, and DH group. The SA lifetime takes the smaller one of the two proposals’ SA lifetime settings.

To configure an IKE proposal:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ike proposal proposal-number</td>
<td>By default, there is an IKE proposal that is used as the default IKE proposal.</td>
</tr>
</tbody>
</table>
| 3.   | encryption-algorithm
   - In non-FIPS mode: encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des-cbc }
   - In FIPS mode: encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 } | By default:  
   - In non-FIPS mode, an IKE proposal uses the 56-bit DES encryption algorithm in CBC mode.  
   - In FIPS mode, an IKE proposal uses the 128-bit AES encryption algorithm in CBC mode. |
| 4.   | authentication-method
   - dsa-signature | pre-share | rsa-signature | By default, an IKE proposal uses the pre-shared key authentication method. |
## Configuring an IKE keychain

Perform this task when you configure the IKE to use the pre-shared key for authentication.

Follow these guidelines when you configure an IKE keychain:

1. Two peers must be configured with the same pre-shared key to pass pre-shared key authentication.

2. You can specify the local address configured in IPsec policy or IPsec policy template view (using the `local-address` command) for the IKE keychain to be applied. If no local address is configured, specify the IP address of the interface to which the IPsec policy is applied.

3. You can specify a priority number for the IKE keychain. To determine the priority of an IKE keychain:
   a. The device examines the existence of the `match local address` command. An IKE keychain with the `match local address` command configured has a higher priority.
   b. If a tie exists, the device compares the priority numbers. An IKE keychain with a smaller priority number has a higher priority.
   c. If a tie still exists, the device prefers an IKE keychain configured earlier.

To configure the IKE keychain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IKE keychain and enter its view.</td>
<td><code>ike keychain keychain-name [ vpn-instance vpn-name ]</code></td>
</tr>
<tr>
<td>3.</td>
<td>Configure a pre-shared key.</td>
<td>In Release 1111: <code>pre-shared-key { address }</code></td>
</tr>
</tbody>
</table>

---

### Table

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Specify an authentication algorithm for the IKE proposal.</td>
<td>In Release 1111: • In non-FIPS mode: `authentication-algorithm { md5</td>
</tr>
<tr>
<td>6.</td>
<td>Specify a DH group for key negotiation in phase 1.</td>
<td>In non-FIPS mode: `dh { group1</td>
</tr>
<tr>
<td>7.</td>
<td>Set the IKE SA lifetime for the IKE proposal.</td>
<td><code>sa duration seconds</code></td>
</tr>
</tbody>
</table>
### Configuring the global identity information

Follow these guidelines when you configure the global identity information for the local IKE:

- The global identity can be used by the device for all IKE SA negotiations, and the local identity (set by the `local-identity` command) can be used only by the device that uses the IKE profile.
- When signature authentication is used, you can set any type of the identity information.
- When pre-shared key authentication is used, you cannot set the DN as the identity.

To configure the global identity information:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td><code>ike identity</code> (address</td>
<td>By default, the IP address of the interface to which the IPsec policy or IPsec policy template is applied is used as the IKE identity.</td>
</tr>
<tr>
<td></td>
<td>{ ipv4-address</td>
<td>`ipv6 ipv6-address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 3.   | `ike signature-identity from-certificate` | By default, the local end uses the identity information specified by `local-identity` or `ike identity` for signature authentication. Configure this command when the aggressive mode and signature authentication are used and the device interconnects with a Comware 5-based peer device. Comware 5-
Configuring the IKE keepalive feature

IKE sends keepalive packets to query the liveness of the peer. If the peer is configured with the keepalive timeout time, you must configure the keepalive interval on the local device. If the peer receives no keepalive packets during the timeout time, the IKE SA is deleted along with the IPsec SAs it negotiated.

Follow these guidelines when you configure the IKE keepalive feature:

- Configure IKE DPD instead of the IKE keepalive feature unless IKE DPD is not supported on the peer. The IKE keepalive feature sends keepalives at regular intervals, which consumes network bandwidth and resources.
- The keepalive timeout time configured on the local device must be longer than the keepalive interval configured at the peer. Since it seldom occurs that more than three consecutive packets are lost on a network, you can set the keepalive timeout three times as long as the keepalive interval.

To configure the IKE keepalive feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the IKE SA keepalive interval.</td>
<td>ike keepalive interval seconds</td>
</tr>
<tr>
<td>3.</td>
<td>Set the IKE SA keepalive timeout time.</td>
<td>ike keepalive timeout seconds</td>
</tr>
</tbody>
</table>

Configuring the IKE NAT keepalive feature

If IPsec traffic passes through a NAT device, you must configure the NAT traversal feature. If no packet travels across an IPsec tunnel in a period of time, the NAT sessions are aged and deleted, disabling the tunnel from transmitting data to the intended end. To prevent NAT sessions from being aged, configure the NAT keepalive feature on the IKE gateway behind the NAT device to send NAT keepalive packets to its peer periodically to keep the NAT session alive.

To configure the IKE NAT keepalive feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the IKE NAT keepalive interval.</td>
<td>ike nat-keepalive seconds</td>
</tr>
</tbody>
</table>

Configuring IKE DPD

DPD detects dead peers. It can operate in periodic mode or on-demand mode.

- **Periodic DPD**—Sends a DPD message at regular intervals. It features an earlier detection of dead peers, but consumes more bandwidth and CPU.
• On-demand DPD—Sends a DPD message based on traffic. When the device has traffic to send and is not aware of the liveness of the peer, it sends a DPD message to query the status of the peer. If the device has no traffic to send, it never sends DPD messages. As a best practice, use the on-demand mode.

The IKE DPD works as follows:
1. The local device sends a DPD message to the peer, and waits for a response from the peer.
2. If the peer does not respond within the retry interval specified by the retry seconds parameter, the local device resends the message.
3. If still no response is received within the retry interval, the local end sends the DPD message again. The system allows a maximum of two retries.
4. If the local device receives no response after two retries, the device considers the peer to be dead, and deletes the IKE SA along with the IPsec SAs it negotiated.
5. If the local device receives a response from the peer during the detection process, the peer is considered alive. The local device performs a DPD detection again when the triggering interval is reached or it has traffic to send, depending on the DPD mode.

Follow these guidelines when you configure the IKE DPD feature:
• When DPD settings are configured in both IKE profile view and system view, the DPD settings in IKE profile view apply. If DPD is not configured in IKE profile view, the DPD settings in system view apply.
• It is a good practice to set the triggering interval longer than the retry interval so that a DPD detection is not triggered during a DPD retry.

To configure IKE DPD:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable sending IKE DPD messages</td>
<td>ike dpd interval-seconds [ retry seconds ] { on-demand</td>
</tr>
</tbody>
</table>

Enabling invalid SPI recovery

An IPsec "black hole" occurs when one IPsec peer fails (for example, a peer can fail if a reboot occurs). One peer fails and loses its SAs with the other peer. When an IPsec peer receives a data packet for which it cannot find an SA, an invalid SPI is encountered. The peer drops the data packet and tries to send an SPI invalid notification to the data originator. This notification is sent by using the IKE SA. Because no IKE SA is available, the notification is not sent. The originating peer continues sending the data by using the IPsec SA that has the invalid SPI, and the receiving peer keeps dropping the traffic.

The invalid SPI recovery feature enables the receiving peer to set up an IKE SA with the originator so that an SPI invalid notification can be sent. Upon receiving the notification, the originating peer deletes the IPsec SA that has the invalid SPI. If the originator has data to send, new SAs will be set up.

Use caution when you enable the invalid SPI recovery feature because using this feature can result in a DoS attack. Attackers can make a great number of invalid SPI notifications to the same peer.

To enable invalid SPI recovery:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Setting the maximum number of IKE SAs

You can set the maximum number of half-open IKE SAs and the maximum number of established IKE SAs.

- The supported maximum number of half-open IKE SAs depends on the device's processing capability. Adjust the maximum number of half-open IKE SAs to make full use of the device's processing capability without affecting the IKE SA negotiation efficiency.
- The supported maximum number of established IKE SAs depends on the device's memory space. Adjust the maximum number of established IKE SAs to make full use of the device's memory space without affecting other applications in the system.

To set the limit on the number of IKE SAs:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the maximum number of half-open IKE SAs and the maximum number of established IKE SAs.</td>
<td>ike limit { max-negotiating-sa negotiation-limit</td>
</tr>
</tbody>
</table>

### Configuring SNMP notifications for IKE

After you enable SNMP notifications for IKE, the IKE module notifies the NMS of important module events. The notifications are sent to the device's SNMP module. You can configure the notification transmission parameters for the SNMP module to specify how the SNMP module displays notifications. For more information about SNMP notifications, see *Network Management and Monitoring Configuration Guide*.

To generate and output SNMP notifications for a specific IKE failure or event type, perform the following tasks:

1. Enable SNMP notifications for IKE globally.
2. Enable SNMP notifications for the failure or event type.

To configure SNMP notifications for IKE:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable SNMP notifications for IKE globally.</td>
<td>snmp-agent trap enable ike global</td>
</tr>
<tr>
<td>3.</td>
<td>Enable SNMP notifications for the specified failure or event types.</td>
<td>snmp-agent trap enable ike [ attr-not-support</td>
</tr>
</tbody>
</table>
### Displaying and maintaining IKE

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display configuration information about all IKE proposals.</td>
<td><code>display ike proposal</code></td>
</tr>
<tr>
<td>Display information about the current IKE SAs.</td>
<td>`display ike sa [ verbose [ connection-id connection-id</td>
</tr>
<tr>
<td>Delete IKE SAs.</td>
<td><code>reset ike sa [ connection-id connection-id ]</code></td>
</tr>
<tr>
<td>Clear IKE MIB statistics.</td>
<td><code>reset ike statistics</code></td>
</tr>
</tbody>
</table>

### IKE configuration examples

#### Main mode IKE with pre-shared key authentication configuration example

**Network requirements**

As shown in Figure 91, configure an IPsec tunnel that uses IKE negotiation between Switch A and Switch B to secure the communication.

Configure Switch A and Switch B to use the default IKE proposal for the IKE negotiation to set up the IPsec SA. Configure the two switches to use the pre-shared key authentication method.

**Figure 91 Network diagram**

![Network diagram](image)

**Configuration procedure**

Make sure Switch A and Switch B can reach each other.

1. Configure Switch A:
   
   ```
   # Assign an IP address to VLAN-interface 1.
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 1
   [SwitchA-vlan-interface1] ip address 1.1.1.1 255.255.0.0
   [SwitchA-vlan-interface1] quit
   # Configure ACL 3101 to identify traffic between Switch A and Switch B.
   [SwitchA] acl number 3101
   [SwitchA-acl-adv-3101] rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
   ```
# Create IPsec transform set tran1.
[SwitchA] ipsec transform-set tran1

# Set the packet encapsulation mode to tunnel.
[SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel

# Use the ESP protocol for the IPsec transform set.
[SwitchA-ipsec-transform-set-tran1] protocol esp

# Specify the encryption and authentication algorithms.
[SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1

# Create IKE keychain keychain1.
[SwitchA] ike keychain keychain1

# Specify 12345zxcvb!@#$%ZXCVB in plain text as the pre-shared key to be used with the remote peer at 2.2.2.2.
[SwitchA-ike-keychain-keychain1] pre-shared-key address 2.2.2.2 255.255.0.0 key simple 12345zxcvb!@#$%ZXCVB

# Create IKE profile profile1.
[SwitchA] ike profile profile1

# Specify IKE keychain keychain1.
[SwitchA-ike-profile-profile1] keychain keychain1

# Configure a peer ID with the identity type of IP address and the value of 2.2.2.2/16.
[SwitchA-ike-profile-profile1] match remote identity address 2.2.2.2 255.255.0.0

# Create an IKE-based IPsec policy entry. Specify the policy name as map1 and set the sequence number to 10.
[SwitchA] ipsec policy map1 10 isakmp

# Specify the remote IP address 2.2.2.2 for the IPsec tunnel.
[SwitchA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2

# Specify ACL 3101 to identify the traffic to be protected.
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101

# Specify IPsec transform set tran1 for the IPsec policy.
[SwitchA-ipsec-policy-isakmp-map1-10] transform-set tran1

# Specify IKE profile profile1 for the IPsec policy.
[SwitchA-ipsec-policy-isakmp-map1-10] ike-profile profile1

# Specify slot 1 as the traffic processing slot for VLAN-interface 1.
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] service slot 1

# Apply IPsec policy map1 to VLAN-interface 1.
[SwitchA-Vlan-interface1] ipsec apply policy map1

2. Configure Switch B:

# Assign an IP address to VLAN-interface 1.
<SwitchB> system-view
[SwitchB] interface Vlan-interface1
[SwitchB-Vlan-interface1] ip address 2.2.2.2 255.255.0.0
# Configure ACL 3101 to identify traffic between Switch B and Switch A.
[SwitchB] acl number 3101
[SwitchB-acl-adv-3101] rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.0 0
[SwitchB-acl-adv-3101] quit

# Create IPsec transform set tran1.
[SwitchB] ipsec transform-set tran1

# Set the packet encapsulation mode to tunnel.
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel

# Use the ESP protocol for the IPsec transform set.
[SwitchB-ipsec-transform-set-tran1] protocol esp

# Specify the encryption and authentication algorithms.
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-192
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-tran1] quit

# Create IKE keychain keychain1.
[SwitchB] ike keychain keychain1

# Specify 12345zxcvb!@#$%ZXCVB in plain text as the pre-shared key to be used with the remote peer at 1.1.1.1.
[SwitchB-ike-keychain-keychain1] pre-shared-key address 1.1.1.1 255.255.0.0 key simple 12345zxcvb!@#$%ZXCVB
[SwitchB-ike-keychain-keychain1] quit

# Create IKE profile profile1.
[SwitchB] ike profile profile1

# Specify IKE keychain keychain1
[SwitchB-ike-profile-profile1] keychain keychain1

# Configure a peer ID with the identity type of IP address and the value of 1.1.1.1/16.
[SwitchB-ike-profile-profile1] match remote identity address 1.1.1.1 255.255.0.0
[SwitchB-ike-profile-profile1] quit

# Create an IKE-based IPsec policy entry. Specify the policy name as use1 and set the sequence number to 10.
[SwitchB] ipsec policy use1 10 isakmp

# Specify the remote IP address 1.1.1.1 for the IPsec tunnel.
[SwitchB-ipsec-policy-isakmp-use1-10] remote-address 1.1.1.1

# Specify ACL 3101 to identify the traffic to be protected.
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101

# Specify IPsec transform set tran1 for the IPsec policy.
[SwitchB-ipsec-policy-isakmp-use1-10] transform-set tran1

# Specify IKE profile profile1 for the IPsec policy.
[SwitchB-ipsec-policy-isakmp-use1-10] ike-profile profile1
[SwitchB-ipsec-policy-isakmp-use1-10] quit

# Specify slot 1 as the traffic processing slot for VLAN-interface 1.
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] service slot 1

# Apply IPsec policy use1 to VLAN-interface 1.
[SwitchB-Vlan-interface1] ipsec apply policy use1
Verifying the configuration

# Initiate a connection from Switch A to Switch B to trigger IKE negotiation. After IPsec SAs are successfully negotiated by IKE, traffic between the two switches is IPsec protected.

Troubleshooting IKE

IKE negotiation failed because no matching IKE proposals were found

Symptom

1. The IKE SA is in Unknown state.
   
   `<Sysname> display ike sa`
   
   
<table>
<thead>
<tr>
<th>Connection-ID</th>
<th>Remote</th>
<th>Flag</th>
<th>DOI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.222.5</td>
<td>Unknown</td>
<td>IPSEC</td>
</tr>
</tbody>
</table>
   
   Flags:
   RD--READY RL--REPLACED FD--FADING

2. When IKE event debugging and packet debugging are enabled, the following messages appear:
   
   IKE event debugging message:
   The attributes are unacceptable.
   
   IKE packet debugging message:
   Construct notification packet: NO_PROPOSAL_CHOSEN.

Analysis

Certain IKE proposal settings are incorrect.

Solution

1. Examine the IKE proposal configuration to see whether the two ends have matching IKE proposals.

2. Modify the IKE proposal configuration to make sure the two ends have matching IKE proposals.

IKE negotiation failed because no IKE proposals or IKE keychains are specified correctly

Symptom

1. The IKE SA is in Unknown state.
   
   `<Sysname> display ike sa`
   
   
<table>
<thead>
<tr>
<th>Connection-ID</th>
<th>Remote</th>
<th>Flag</th>
<th>DOI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>192.168.222.5</td>
<td>Unknown</td>
<td>IPSEC</td>
</tr>
</tbody>
</table>
   
   Flags:
   RD--READY RL--REPLACED FD--FADING

2. The following IKE event debugging or packet debugging message appeared:
   
   IKE event debugging message:
   Notification PAYLOAD_MALFORMED is received.
IKE packet debugging message:
Construct notification packet: PAYLOAD_MALFORMED.

Analysis
- If the following debugging information appeared, the matched IKE profile is not using the matched IKE proposal:
  Failed to find proposal 1 in profile profile1.
- If the following debugging information appeared, the matched IKE profile is not using the matched IKE keychain:
  Failed to find keychain keychain1 in profile profile1.

Solution
- Verify that the matched IKE proposal (IKE proposal 1 in this debugging message example) is specified for the IKE profile (IKE profile 1 in the example).
- Verify that the matched IKE keychain (IKE keychain 1 in this debugging message example) is specified for the IKE profile (IKE profile 1 in the example).

IPsec SA negotiation failed because no matching IPsec transform sets were found

Symptom
1. The display ike sa command shows that the IKE SA negotiation succeeded and the IKE SA is in RD state, but the display ipsec sa command shows that the expected IPsec SA has not been negotiated yet.
2. The following IKE debugging message appeared:
   The attributes are unacceptable.
   Or:
   Construct notification packet: NO_PROPOSAL_CHOSEN.

Analysis
Certain IPsec policy settings are incorrect.

Solution
1. Examine the IPsec configuration to see whether the two ends have matching IPsec transform sets.
2. Modify the IPsec configuration to make sure the two ends have matching IPsec transform sets.

IPsec SA negotiation failed due to invalid identity information

Symptom
1. The display ike sa command shows that the IKE SA negotiation succeeded and the IKE SA is in RD state, but the display ipsec sa command shows that the expected IPsec SA has not been negotiated yet.
2. The following IKE debugging message appeared:
   Notification INVALID_ID_INFORMATION is received.
   Or:
   Failed to get IPsec policy when renegotiating IPsec SA. Delete IPsec SA.
   Construct notification packet: INVALID_ID_INFORMATION.
Analysis

Certain IPsec policy settings of the responder are incorrect. Verify the settings as follows:

1. Use the `display ike sa verbose` command to verify that matching IKE profiles were found in IKE negotiation phase 1. If no matching IKE profiles were found and the IPsec policy has an IKE profile specified, the IPsec SA negotiation fails.

# Verify that matching IKE profiles were found in IKE negotiation phase 1.

```
<Sysname> display ike sa verbose
-----------------------------------------------
Connection ID: 3
Outside VPN:
Inside VPN:
Profile:
  Transmitting entity: Responder
-----------------------------------------------
Local IP: 192.168.222.5
Local ID type: IPV4_ADDR
Local ID: 192.168.222.5
Remote IP: 192.168.222.71
Remote ID type: IPV4_ADDR
Remote ID: 192.168.222.71
Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: MD5
Encryption-algorithm: 3DES-CBC
Life duration(sec): 86400
Remaining key duration(sec): 85847
Exchange-mode: Main
Diffie-Hellman group: Group 1
NAT traversal: Not detected
```

# Verify that the IPsec policy has an IKE profile specified.

```
<Sysname> display ipsec policy
-------------------------------------------
IPsec Policy: policy1
Interface: Vlan-interface1
-------------------------------------------
Sequence number: 1
Mode: isakmp
Description:
Security data flow: 3000
Selector mode: aggregation
Local address: 192.168.222.5
Remote address: 192.168.222.71
Transform set: transform1
```
IKE profile: profile1
SA duration (time based):
SA duration (traffic based):
SA idle time:

2. Verify that the ACL used by the IPsec policy is correctly configured. If the flow range defined by the responder’s ACL is smaller than that defined by the initiator’s ACL, IPsec proposal matching will fail.

For example, if the initiator’s ACL defines a flow from one network segment to another but the responder’s ACL defines a flow from one host to another host, IPsec proposal matching will fail.

# On the initiator:

[Sysname] display acl 3000
Advanced ACL 3000, named -none-, 2 rules,
ACL's step is 5
rule 0 permit ip source 192.168.222.0 0.0.0.255 destination 192.168.222.0 0.0.0.255

# On the responder:

[Sysname] display acl 3000
Advanced ACL 3000, named -none-, 2 rules,
ACL's step is 5
rule 0 permit ip source 192.168.222.71 0 destination 192.168.222.5 0

3. Verify that the IPsec policy has a remote address and an IPsec transform set configured and that the IPsec transform set has all necessary settings configured.

If, for example, the IPsec policy has no remote address configured, the IPsec SA negotiation will fail:

[Sysname] display ipsec policy

-------------------------------------------
IPsec Policy: policy1
Interface: Vlan-interface1
-------------------------------------------

Sequence number: 1
Mode: isakmp
Description:
Security data flow: 3000
Selector mode: aggregation
Local address: 192.168.222.5
Remote address:
Transform set: transform1
IKE profile: profile1
SA duration (time based):
SA duration (traffic based):
SA idle time:

Solution

1. If no matching IKE profiles were found and the IPsec policy has an IKE profile specified, remove the specified IKE profile from the IPsec policy.

2. If the flow range defined by the responder’s ACL is smaller than that defined by the initiator’s ACL, modify the responder’s ACL so the ACL defines a flow range equal to or greater than that of the initiator’s ACL.
For example:

```
[Sysname] display acl 3000
Advanced ACL 3000, named -none-, 2 rules,
ACL's step is 5
  rule 0 permit ip source 192.168.222.0 0.0.0.255 destination 192.168.222.0 0.0.0.255
```

3. Configure the missing settings (for example, the remote address).
Configuring IKEv2

Overview

Internet Key Exchange version 2 (IKEv2) is an enhanced version of IKEv1. The same as IKEv1, IKEv2 has a set of self-protection mechanisms and can be used on insecure networks for reliable identity authentication, key distribution, and IPsec SA negotiation. IKEv2 provides stronger protection against attacks and higher key exchange ability and needs fewer message exchanges than IKEv1.

IKEv2 negotiation process

Compared with IKEv1, IKEv2 simplifies the negotiation process and is much more efficient.
IKEv2 defines three types of exchanges: initial exchanges, CREATE_CHILD_SA exchange, and INFORMATIONAL exchange.

As shown in Figure 92, IKEv2 uses two exchanges during the initial exchange process: IKE_SA_INIT and IKE_AUTH, each with two messages.

- **IKE_SA_INIT exchange**—Negotiates IKE SA parameters and exchanges keys.
- **IKE_AUTH exchange**—Authenticates the identity of the peer and establishes IPsec SAs.

After the four-message initial exchanges, IKEv2 sets up one IKE SA and one pair of IPsec SAs. For IKEv1 to set up one IKE SA and one pair of IPsec SAs, it must go through two phases that use a minimum of six messages.

To set up one more pair of IPsec SAs within the IKE SA, IKEv2 goes on to perform an additional two-message exchange—the CREATE_CHILD_SA exchange. One CREATE_CHILD_SA exchange creates one pair of IPsec SAs. IKEv2 also uses the CREATE_CHILD_SA exchange to rekey IKE SAs and Child SAs.

IKEv2 uses the INFORMATIONAL exchange to convey control messages about errors and notifications.

**Figure 92 IKEv2 Initial exchange process**
New features in IKEv2

DH guessing

In the IKE_SA_INIT exchange, the initiator guesses the DH group that the responder is most likely to use and sends it in an IKE_SA_INIT request message. If the initiator's guess is correct, the responder responds with an IKE_SA_INIT response message and the IKE_SA_INIT exchange is finished. If the guess is wrong, the responder responds with an INVALID_KE_PAYLOAD message that contains the DH group that it wants to use. The initiator then uses the DH group selected by the responder to reinitiate the IKE_SA_INIT exchange. The DH guessing mechanism allows for more flexible DH group configuration and enables the initiator to adapt to different responders.

Cookie challenging

Messages for the IKE_SA_INIT exchange are in plain text. An IKEv1 responder cannot confirm the validity of the initiators and must maintain half-open IKE SAs, which makes the responder susceptible to DoS attacks. An attacker can send a large number of IKE_SA_INIT requests with forged source IP addresses to the responder, exhausting the responder's system resources.

IKEv2 introduces the cookie challenging mechanism to prevent such DoS attacks. When an IKEv2 responder maintains a threshold number of half-open IKE SAs, it starts the cookie challenging mechanism. The responder generates a cookie and includes it in the response sent to the initiator. If the initiator initiates a new IKE_SA_INIT request that carries the correct cookie, the responder considers the initiator valid and proceeds with the negotiation. If the carried cookie is incorrect, the responder terminates the negotiation.

The cookie challenging mechanism automatically stops working when the number of half-open IKE SAs drops below the threshold.

IKEv2 SA rekeying

For security purposes, both IKE SAs and IPsec SAs have a lifetime and must be rekeyed when the lifetime expires. An IKEv1 SA lifetime is negotiated. An IKEv2 SA lifetime, in contrast, is configured. If two peers are configured with different lifetimes, the peer with the shorter lifetime always initiates the SA rekeying. This mechanism reduces the possibility that two peers will simultaneously initiate a rekeying. Simultaneous rekeying results in redundant SAs and SA status inconsistency on the two peers.

IKEv2 message retransmission

Unlike IKEv1 messages, IKEv2 messages appear in request/response pairs. IKEv2 uses the Message ID field in the message header to identify the request/response pair. If an initiator sends a request but receives no response with the same Message ID value within a specific period of time, the initiator retransmits the request.

It is always the IKEv2 initiator that initiates the retransmission, and the retransmitted message must use the same Message ID value.

Protocols and standards

- RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 4306, Internet Key Exchange (IKEv2) Protocol
- RFC 4718, IKEv2 Clarifications and Implementation Guidelines
- RFC 2412, The OAKLEY Key Determination Protocol
- RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2)

Feature and software version compatibility

The IKEv2 feature is available in Release 1121 and later.
IKEv2 configuration task list

Determine the following parameters prior to IKEv2 configuration:

- The strength of the algorithms for IKEv2 negotiation, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups. Different algorithms provide different levels of protection. A stronger algorithm means better resistance to decryption of protected data but requires more resources. Typically, the longer the key, the stronger the algorithm.

- The local and remote identity authentication methods.
  - To use the pre-shared key authentication method, you must determine the pre-shared key.
  - To use the RSA digital signature authentication method, you must determine the PKI domain for the local end to use. For information about PKI, see "Configuring PKI."

To configure IKEv2, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring an IKEv2 profile</td>
<td>N/A</td>
</tr>
<tr>
<td>(Required.) Configuring an IKEv2 policy</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Configuring an IKEv2 proposal</td>
<td>If you specify an IKEv2 proposal in an IKEv2 policy, you must configure the IKEv2 proposal.</td>
</tr>
<tr>
<td>Configuring an IKEv2 keychain</td>
<td>Required when either end or both ends use the pre-shared key authentication method.</td>
</tr>
<tr>
<td>Configure global IKEv2 parameters</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Enabling the cookie challenging feature</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring the IKEv2 DPD feature</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Configuring the IKEv2 NAT keepalive feature</td>
<td></td>
</tr>
<tr>
<td>The cookie challenging feature takes effect only on IKEv2 responders.</td>
<td></td>
</tr>
</tbody>
</table>

Configuring an IKEv2 profile

An IKEv2 profile is intended to provide a set of parameters for IKEv2 negotiation. To configure an IKEv2 profile, perform the following tasks:

1. Specify the local and remote identity authentication methods.
   The local and remote identity authentication methods must both be specified and they can be different. You can specify only one local identity authentication method and multiple remote identity authentication methods.

2. Configure the IKEv2 keychain or PKI domain for the IKEv2 profile to use:
   - To use digital signature authentication, configure a PKI domain.
   - To use pre-shared key authentication, configure an IKEv2 keychain.

3. Configure the local ID, the ID that the device uses to identify itself to the peer during IKEv2 negotiation:
   - For digital signature authentication, the device can use an ID of any type. If the local ID is an IP address that is different from the IP address in the local certificate, the device uses the FQDN as the local ID. The FQDN is the device name configured by using the `sysname` command.
   - For pre-shared key authentication, the device can use an ID of any type other than the DN.

4. Configure peer IDs.
The device compares the received peer ID with the peer IDs of its local IKEv2 profiles. If a match is found, it uses the IKEv2 profile with the matching peer ID for IKEv2 negotiation. IKEv2 profiles will be compared in descending order of their priorities.

5. Specify a local interface or IP address for the IKEv2 profile so the profile can be applied only to the specified interface or IP address. For this task, specify the local address configured in IPsec policy or IPsec policy template view (using the `local-address` command). If no local address is configured, specify the IP address of the interface that uses the IPsec policy.

6. Specify a priority number for the IKEv2 profile. To determine the priority of an IKEv2 profile:
   a. First, the device examines the existence of the `match local` command. An IKEv2 profile with the `match local` command configured has a higher priority.
   b. If a tie exists, the device compares the priority numbers. An IKEv2 profile with a smaller priority number has a higher priority.
   c. If a tie still exists, the device prefers an IKEv2 profile configured earlier.

7. Specify a VPN instance for the IKEv2 profile. The IKEv2 profile is used for IKEv2 negotiation only on the interfaces that belong to the VPN instance.

8. Configure the IKEv2 SA lifetime.
   The local and remote ends can use different IKEv2 SA lifetimes. They do not negotiate the lifetime. The end with a smaller SA lifetime will initiate an SA negotiation when the lifetime expires.

9. Configure IKEv2 DPD to detect dead IKEv2 peers. You can also configure this feature in system view. If you configure IKEv2 DPD in both views, the IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

10. Specify an inside VPN instance. This setting determines where the device should forward received IPsec packets after it de-encapsulates them. If you specify an inside VPN instance, the device looks for a route in the specified VPN instance to forward the packets. If you do not specify an inside VPN instance, the internal and external networks are in the same VPN instance. The device looks for a route in this VPN instance to forward the packets.

11. Configure the NAT keepalive interval.
    Configure this task when the device is behind a NAT gateway. The device sends NAT keepalive packets regularly to its peer to prevent the NAT session from being aged because of no matching traffic.

12. Enable the configuration exchange feature.
    The configuration exchange feature enables the local and remote ends to exchange configuration data, such as gateway address, internal IP address, and route. The exchange includes data request and response, and data push and response.
    This feature typically applies to scenarios where branches and the headquarters communicate through virtual tunnels.
    This feature enables the IPsec gateway at a branch to send IP address requests to the IPsec gateway at the headquarters. When the headquarters receives the request, it sends an IP address to the branch in the response packet. The headquarters can also actively push an IP address to the branch. The branch uses the allocated IP address as the IP address of the virtual tunnel to communicate with the headquarters.

To configure an IKEv2 profile:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IKEv2 profile and enter IKEv2 profile view.</td>
<td>ikev2 profile profile-name</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the local and authentication-method { local }</td>
<td>By default, no local or remote identity</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1.</td>
<td>remote</td>
<td>remote identity authentication methods.</td>
</tr>
<tr>
<td>2.</td>
<td>{ dsa-signature</td>
<td>ecdsa-signature</td>
</tr>
<tr>
<td>4.</td>
<td>Specify a keychain.</td>
<td>keychain keychain-name By default, no keychain is specified for an IKEv2 profile. Perform this task when the pre-shared key authentication method is specified.</td>
</tr>
<tr>
<td>5.</td>
<td>Specify a PKI domain.</td>
<td>certificate domain domain-name [ sign</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the local ID.</td>
<td>identity local { address { ipv4-address</td>
</tr>
<tr>
<td>7.</td>
<td>Configure peer IDs.</td>
<td>match remote { certificate policy-name</td>
</tr>
<tr>
<td>8.</td>
<td>(Optional.) Specify the local interface or IP address to which the IKEv2 profile can be applied.</td>
<td>match local address { interface-type interface-number</td>
</tr>
<tr>
<td>9.</td>
<td>(Optional.) Specify a priority for the IKEv2 profile.</td>
<td>priority priority By default, the priority of an IKEv2 profile is 100.</td>
</tr>
<tr>
<td>10.</td>
<td>(Optional.) Specify a VPN instance for the IKEv2 profile.</td>
<td>match vrf { name vrf-name</td>
</tr>
<tr>
<td>11.</td>
<td>(Optional.) Set the IKEv2 SA lifetime for the IKEv2 profile.</td>
<td>sa duration seconds By default, the IKEv2 SA lifetime is 86400 seconds.</td>
</tr>
<tr>
<td>12.</td>
<td>(Optional.) Configure the DPD feature for the IKEv2 profile.</td>
<td>dpd interval interval [ retry seconds ] { on-demand</td>
</tr>
<tr>
<td>13.</td>
<td>(Optional.) Specify an inside VPN instance for the IKEv2 profile.</td>
<td>inside-vrf vrf-name By default, no inside VPN instance is specified for an IKEv2 profile. The internal and external networks are in the same VPN instance. The device forwards protected data to this VPN instance.</td>
</tr>
<tr>
<td>14.</td>
<td>(Optional.) Set the IKEv2 NAT keepalive</td>
<td>nat-keepalive seconds By default, the global IKEv2 NAT keepalive setting is used.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>interval.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15. (Optional.) Enable the configuration exchange feature.</td>
<td>config-exchange { request</td>
<td>set { accept</td>
</tr>
</tbody>
</table>

**Configuring an IKEv2 policy**

During the IKE_SA_INIT exchange, each end tries to find a matching IKEv2 policy, using the IP address of the local security gateway as the matching criterion.

- If IKEv2 policies are configured, IKEv2 searches for an IKEv2 policy that uses the IP address of the local security gateway. If no IKEv2 policy uses the IP address or the policy is using an incomplete proposal, the IKE_SA_INIT exchange fails.
- If no IKEv2 policy is configured, IKEv2 uses the system default IKEv2 policy `default`.

The device matches IKEv2 policies in the descending order of their priorities. To determine the priority of an IKEv2 policy:

1. First, the device examines the existence of the `match local address` command. An IKEv2 policy with the `match local address` command configured has a higher priority.
2. If a tie exists, the device compares the priority numbers. An IKEv2 policy with a smaller priority number has a higher priority.
3. If a tie still exists, the device prefers an IKEv2 policy configured earlier.

To configure an IKEv2 policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IKEv2 policy and enter IKEv2 policy view.</td>
<td>ikev2 policy <code>policy-name</code></td>
</tr>
<tr>
<td>3.</td>
<td>Specify the local interface or address used for IKEv2 policy matching.</td>
<td>`match local address { interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Specify a VPN instance for IKEv2 policy matching.</td>
<td>`match vrf { name vrf-name</td>
</tr>
<tr>
<td>5.</td>
<td>Specify an IKEv2 proposal for the IKEv2 policy.</td>
<td>proposal <code>proposal-name</code></td>
</tr>
<tr>
<td>6.</td>
<td>Specify a priority for the IKEv2 policy.</td>
<td><code>priority priority</code></td>
</tr>
</tbody>
</table>

**Configuring an IKEv2 proposal**

An IKEv2 proposal contains security parameters used in IKE_SA_INIT exchanges, including the encryption algorithms, integrity protection algorithms, PRF algorithms, and DH groups. An algorithm specified earlier has a higher priority.
A complete IKEv2 proposal must have at least one set of security parameters, including one encryption algorithm, one integrity protection algorithm, one PRF algorithm, and one DH group.

You can specify multiple IKEv2 proposals for an IKEv2 policy. A proposal specified earlier has a higher priority.

To configure an IKEv2 proposal:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IKEv2 proposal and enter IKEv2 proposal view.</td>
<td>ikev2 proposal <em>proposal-name</em></td>
</tr>
<tr>
<td>4.</td>
<td>Specify the integrity protection algorithms.</td>
<td>In non-FIPS mode:&lt;br&gt;integrity { aes-xcbc-mac</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the PRF algorithms.</td>
<td>In non-FIPS mode:&lt;br&gt;prf { aes-xcbc-mac</td>
</tr>
</tbody>
</table>
### Configuring an IKEv2 keychain

An IKEv2 keychain specifies the pre-shared keys used for IKEv2 negotiation.

An IKEv2 keychain can have multiple IKEv2 peers. Each peer has a symmetric pre-shared key or an asymmetric pre-shared key pair, and information for identifying the peer (such as the peer's host name, IP address or address range, or ID).

An IKEv2 negotiation initiator uses the peer host name or IP address/address range as the matching criterion to search for a peer. A responder uses the peer host IP address/address range or ID as the matching criterion to search for a peer.

To configure an IKEv2 keychain:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an IKEv2 keychain and enter IKEv2 keychain view.</td>
<td>ikev2 keychain keychain-name</td>
</tr>
<tr>
<td>3.</td>
<td>Create an IKEv2 peer and enter IKEV2 peer view.</td>
<td>peer name</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the information for identifying the IKEv2 peer.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To configure a host name for the peer: hostname host-name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To configure a host IP address or address range for the peer: address { ipv4-address [ mask</td>
<td>mask-length ]</td>
</tr>
<tr>
<td></td>
<td>• To configure an ID for the peer: identity { address { ipv4-address</td>
<td>ipv6 { ipv6-address } }</td>
</tr>
<tr>
<td>5.</td>
<td>Configure a pre-shared key for the peer.</td>
<td>pre-shared-key [ local</td>
</tr>
</tbody>
</table>
Configure global IKEv2 parameters

Enabling the cookie challenging feature

Enable cookie challenging on responders to protect them against DoS attacks that use a large number of source IP addresses to forge IKE_SA_INIT requests.

To enable cookie challenging:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable IKEv2 cookie challenging.</td>
<td>ikev2 cookie-challenge number</td>
</tr>
</tbody>
</table>

Configuring the IKEv2 DPD feature

IKEv2 DPD detects dead IKEv2 peers in periodic or on-demand mode.

- **Periodic IKEv2 DPD**—Verifies the liveness of an IKEv2 peer by sending DPD messages at regular intervals.
- **On-demand IKEv2 DPD**—Verifies the liveness of an IKEv2 peer by sending DPD messages before sending data.
  - Before the device sends data, it identifies the time interval for which the last IPsec packet has been received from the peer. If the time interval exceeds the DPD interval, it sends a DPD message to the peer to detect its liveness.
  - If the device has no data to send, it never sends DPD messages.

If you configure IKEv2 DPD in both IKEv2 profile view and system view, the IKEv2 DPD settings in IKEv2 profile view apply. If you do not configure IKEv2 DPD in IKEv2 profile view, the IKEv2 DPD settings in system view apply.

To configure global IKEv2 DPD:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure global IKEv2 DPD.</td>
<td>ikev2 dpd interval interval [ retry seconds ] { on-demand</td>
</tr>
</tbody>
</table>

Configuring the IKEv2 NAT keepalive feature

Configure this feature on the IKEv2 gateway behind the NAT device. The gateway then sends NAT keepalive packets regularly to its peer to keep the NAT session alive, so that the peer can access the device.

The NAT keepalive interval must be shorter than the NAT session lifetime.

This feature takes effect after the device detects the NAT device.

To configure the IKEv2 NAT keepalive feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
### Displaying and maintaining IKEv2

**Task**
- Display the IKEv2 proposal configuration.
  
  **Command**
  ```
  display ikev2 proposal [ name | default ]
  ```

- Display the IKEv2 policy configuration.
  
  **Command**
  ```
  display ikev2 policy [ policy-name | default ]
  ```

- Display the IKEv2 profile configuration.
  
  **Command**
  ```
  display ikev2 profile [ profile-name ]
  ```

- Display the IKEv2 SA information.
  
  **Command**
  ```
  display ikev2 sa [ { count | local | remote } { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] ] [ verbose [ tunnel tunnel-id ] ]
  ```

- Delete IKEv2 SAs and the child SAs negotiated through the IKEv2 SAs.
  
  **Command**
  ```
  reset ikev2 sa [ [ { local | remote } { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] ] [ tunnel tunnel-id ] ]
  ```

### IKEv2 configuration examples

#### IKEv2 with pre-shared key authentication configuration example

**Network requirements**

As shown in **Figure 93**, configure an IKE-based IPsec tunnel between Switch A and Switch B to secure the communication between the switches.

- Configure Switch A and Switch B to use the default IKEv2 proposal and the default IKEv2 policy in IKEv2 negotiation to set up IPsec SAs.
- Configure the two switches to use the pre-shared key authentication method in IKEv2 negotiation.

**Figure 93 Network diagram**

![Network Diagram](image)

**Configuration procedures**

1. **Configure Switch A:**

   ```
   # Assign an IP address to VLAN-interface 1.
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 1
   [SwitchA-vlan-interface1] ip address 1.1.1.1 255.255.255.0
   [SwitchA-vlan-interface1] quit
   ```
# Configure IPv4 advanced ACL 3101 to identify traffic between Switch A and Switch B.

```
[SwitchA] acl advanced 3101
[SwitchA-acl-ipv4-adv-3101] rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
[SwitchA-acl-ipv4-adv-3101] quit
```

# Create an IPsec transform set named tran1.

```
[SwitchA] ipsec transform-set tran1
```

# Set the packet encapsulation mode to tunnel.

```
[SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

# Use the ESP protocol for the IPsec transform set.

```
[SwitchA-ipsec-transform-set-tran1] protocol esp
```

# Specify the encryption and authentication algorithms.

```
[SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-transform-set-tran1] quit
```

# Create an IKEv2 keychain named keychain1.

```
[SwitchA] ikev2 keychain keychain1
```

# Create an IKEv2 peer named peer1.

```
[SwitchA-ikev2-keychain-keychain1] peer peer1
```

# Specify peer IP address 2.2.2.2/24.

```
[SwitchA-ikev2-keychain-keychain1-peer-peer1] address 2.2.2.2 24
```

# Specify the peer ID, which is IP address 2.2.2.2.

```
[SwitchA-ikev2-keychain-keychain1-peer-peer1] identity address 2.2.2.2
```

# Specify abcde in plain text as the pre-shared key to be used with the peer at 2.2.2.2.

```
[SwitchA-ikev2-keychain-keychain1-peer-peer1] pre-shared-key plaintext abcde
[SwitchA-ikev2-keychain-keychain1-peer-peer1] quit
```

# Create an IKEv2 profile named profile1.

```
[SwitchA] ikev2 profile profile1
```

# Specify the local authentication method as pre-shared key.

```
[SwitchA-ikev2-profile-profile1] authentication-method local pre-share
```

# Specify the remote authentication method as pre-shared key.

```
[SwitchA-ikev2-profile-profile1] authentication-method remote pre-share
```

# Specify IKEv2 keychain keychain1.

```
[SwitchA-ikev2-profile-profile1] keychain keychain1
```

# Specify the peer ID that the IKEv2 profile matches. The peer ID is IP address 2.2.2.2/24.

```
[SwitchA-ikev2-profile-profile1] match remote identity address 2.2.2.2 255.255.255.0
[SwitchA-ikev2-profile-profile1] quit
```

# Create an IKE-based IPsec policy entry. Specify the policy name as map1 and set the sequence number to 10.

```
[SwitchA] ipsec policy map1 10 isakmp
```

# Specify remote IP address 2.2.2.2 for the IPsec tunnel.

```
[SwitchA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2
```

# Specify ACL 3101 to identify the traffic to be protected.

```
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
```

# Specify IPsec transform set tran1 for the IPsec policy.

```
[SwitchA-ipsec-policy-isakmp-map1-10] transform-set tran1
```

# Specify IKEv2 profile profile1 for the IPsec policy.
2. Configure Switch B:

   # Assign an IP address to VLAN-interface 1.
   <SwitchB> system-view
   [SwitchB] interface Vlan-interface1
   [SwitchB-Vlan-interface1] ip address 2.2.2.2 255.255.255.0
   [SwitchB-Vlan-interface1] quit

   # Configure IPv4 advanced ACL 3101 to identify traffic between Switch A and Switch B.
   [SwitchB] acl advanced 3101
   [SwitchB-acl-ipv4-adv-3101] rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.0 0
   [SwitchB-acl-ipv4-adv-3101] quit

   # Create an IPsec transform set named tran1.
   [SwitchB] ipsec transform-set tran1

   # Set the packet encapsulation mode to tunnel.
   [SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel

   # Use the ESP protocol for the IPsec transform set.
   [SwitchB-ipsec-transform-set-tran1] protocol esp

   # Specify the encryption and authentication algorithms.
   [SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
   [SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
   [SwitchB-ipsec-transform-set-tran1] quit

   # Create an IKEv2 keychain named keychain1.
   [SwitchB] ikev2 keychain keychain1

   # Create an IKEv2 peer named peer1.
   [SwitchB-ikev2-keychain-keychain1] peer peer1

   # Specify peer IP address 1.1.1.1/24.
   [SwitchB-ikev2-keychain-keychain1-peer-peer1] address 1.1.1.1 24

   # Specify the peer ID, which is IP address 1.1.1.1.
   [SwitchB-ikev2-keychain-keychain1-peer-peer1] identity address 1.1.1.1

   # Specify abcde in plain text as the pre-shared key to be used with the peer at 1.1.1.1.
   [SwitchB-ikev2-keychain-keychain1-peer-peer1] pre-shared-key plaintext abcde
   [SwitchB-ikev2-keychain-keychain1-peer-peer1] quit
   [SwitchB-ikev2-keychain-keychain1] quit

   # Create an IKEv2 profile named profile1.
   [SwitchB] ikev2 profile profile1

   # Specify the local authentication method as pre-shared key.
   [SwitchB-ikev2-profile-profile1] authentication-method local pre-share

   # Specify the remote authentication method as pre-shared key.
   [SwitchB-ikev2-profile-profile1] authentication-method remote pre-share

   # Specify IKEv2 keychain keychain1.
   [SwitchB-ikev2-profile-profile1] keychain keychain1

   # Specify the peer ID that the IKEv2 profile matches. The peer ID is IP address 1.1.1.1/24.
network requirements

as shown in figure 94, configure an ike-based ipsec tunnel between switch a and switch b to secure the communication between the switches.

configure switch a and switch b to use ikev2 negotiation and rsa signature authentication.

figure 94 network diagram

configuration procedure

1. configure switch a:
   # assign an ip address to vlan-interface 1.
   <switcha> system-view
   [switcha] interface vlan-interface 1
   [switcha-vlan-interface1] ip address 1.1.1.1 255.255.255.0
# Configure IPv4 advanced ACL 3101 to identify traffic between Switch A and Switch B.

```
[SwitchA] acl advanced 3101
[SwitchA-acl-ipv4-adv-3101] rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
```

# Create an IPsec transform set named tran1.

```
[SwitchA] ipsec transform-set tran1
```

# Set the packet encapsulation mode to tunnel.

```
[SwitchA-ipsec-transform-set-tran1] encapsulation-mode tunnel
```

# Use the ESP protocol for the IPsec transform set.

```
[SwitchA-ipsec-transform-set-tran1] protocol esp
```

# Specify the encryption and authentication algorithms.

```
[SwitchA-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[SwitchA-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-transform-set-tran1] quit
```

# Create a PKI entity named entity1.

```
[SwitchA] pki entity entity1
```

# Set the common name to switcha for the PKI entity.

```
[SwitchA-pki-entity-entity1] common-name switcha
[SwitchA-pki-entity-entity1] quit
```

# Create a PKI domain named domain1.

```
[SwitchA] pki domain domain1
```

# Set the certificate request mode to auto and set the password to 123 for certificate revocation.

```
[SwitchA-pki-domain-domain1] certificate request mode auto password simple 123
```

# Set an MD5 fingerprint for verifying the validity of the CA root certificate.

```
[SwitchA-pki-domain-domain1] root-certificate fingerprint md5 50c7a2d282ea710a449eede6c56b102e
```

# Specify the trusted CA 8088.

```
[SwitchA-pki-domain-domain1] ca identifier 8088
```

# Specify the URL of the registration server for certificate request through the SCEP protocol. This example uses http://192.168.222.1:446/eadbf9af4f2c4641e685f7a6021e7b298373feb7.

```
[SwitchA-pki-domain-domain1] certificate request url http://192.168.222.1:446/eadbf9af4f2c4641e685f7a6021e7b298373feb7
```

# Specify the CA to accept certificate requests.

```
[SwitchA-pki-domain-domain1] certificate request from ca
```

# Specify the PKI entity for certificate request as entity1.

```
[SwitchA-pki-domain-domain1] certificate request entity entity1
```

# Specify RSA key pair rsa1 with the general purpose for certificate request.

```
[SwitchA-pki-domain-domain1] public-key rsa general name rsa1
[SwitchA-pki-domain-domain1] quit
```

# Create an IKEv2 profile named profile1.

```
[SwitchA] ikev2 profile profile1
```

# Specify the local authentication method as RSA signatures.

```
[SwitchA-ikev2-profile-profile1] authentication-method local rsa-signature
```

# Specify the remote authentication method as RSA signatures.

```
[SwitchA-ikev2-profile-profile1] authentication-method remote rsa-signature
```

# Specify PKI domain domain1 for the IKEv2 profile.
Configure Switch A:

1. Set the local ID to FQDN name `www.switcha.com`.

   [SwitchA-ikev2-profile-profile1] identity local fqdn www.switcha.com

2. Specify the peer ID that the IKEv2 profile matches. The peer ID is FQDN name `www.routerb.com`.

   [SwitchA-ikev2-profile-profile1] match remote identity fqdn www.routerb.com

3. Create an IKEv2 proposal named `10`.

   [SwitchA] ikev2 proposal 10

4. Specify the integrity protection algorithm as HMAC-MD5.

   [SwitchA-ikev2-proposal-10] integrity md5

5. Specify the encryption algorithm as 3DES-CBC.

   [SwitchA-ikev2-proposal-10] encryption 3des-cbc

6. Specify the DH group as Group 1.

   [SwitchA-ikev2-proposal-10] dh group1

7. Specify the PRF algorithm as HMAC-MD5.

   [SwitchA-ikev2-proposal-10] prf md5

8. Create an IKEv2 policy named `1`.

   [SwitchA] ikev2 policy 1

9. Specify IKEv2 proposal `10` for the IKEv2 policy.

   [SwitchA-ikev2-policy-1] proposal 10

10. Create an IKE-based IPsec policy entry. Specify the policy name as `map1` and set the sequence number to 10.

    [SwitchA] ipsec policy map1 10 isakmp

11. Specify remote IP address 2.2.2.2 for the IPsec tunnel.

    [SwitchA-ipsec-policy-isakmp-map1-10] remote-address 2.2.2.2

12. Specify IPsec transform set `tran1` for the IPsec policy.

    [SwitchA-ipsec-policy-isakmp-map1-10] transform-set tran1

13. Specify ACL 3101 to identify the traffic to be protected.

    [SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101

14. Specify IKEv2 profile `profile1` for the IPsec policy.

    [SwitchA-ipsec-policy-isakmp-map1-10] ikev2-profile profile1

15. Apply IPsec policy `map1` to VLAN-interface 1.

    [SwitchA-Vlan-interface1] ipsec apply policy map1

2. Configure Switch B:

   # Assign an IP address to VLAN-interface 1.

   <SwitchB> system-view

   [SwitchB] interface Vlan-interface1

   [SwitchB-Vlan-interface1] ip address 2.2.2.2 255.255.255.0

   # Configure IPv4 advanced ACL 3101 to identify traffic between Switch A and Switch B.

   [SwitchB] acl advanced 3101
[SwitchB-acl-ipv4-adv-3101] rule 0 permit ip source 2.2.2.2 0 destination 1.1.1.0 0
[SwitchB-acl-ipv4-adv-3101] quit

# Create an IPsec transform set named tran1.
[SwitchB] ipsec transform-set tran1

# Set the packet encapsulation mode to tunnel.
[SwitchB-ipsec-transform-set-tran1] encapsulation-mode tunnel

# Use the ESP protocol for the IPsec transform set.
[SwitchB-ipsec-transform-set-tran1] protocol esp

# Specify the encryption and authentication algorithms.
[SwitchB-ipsec-transform-set-tran1] esp encryption-algorithm des-cbc
[SwitchB-ipsec-transform-set-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-transform-set-tran1] quit

# Create a PKI entity named entity2.
[SwitchB] pki entity entity2

# Set the common name to routerb for the PKI entity.
[SwitchB-pki-entity-entity2] common-name routerb
[SwitchB-pki-entity-entity2] quit

# Create a PKI domain named domain2.
[SwitchB] pki domain domain2

# Set the certificate request mode to auto and set the password to 123 for certificate revocation.
[SwitchB-pki-domain-domain2] certificate request mode auto password simple 123

# Set an MD5 fingerprint for verifying the validity of the CA root certificate.
[SwitchB-pki-domain-domain2] root-certificate fingerprint md5 50c7a2d282ea710a449eede6c56b102e

# Specify the trusted CA 8088.
[SwitchB-pki-domain-domain2] ca identifier 8088

# Specify the URL of the registration server for certificate request through the SCEP protocol. This example uses http://192.168.222.1:446/eadbf9af4f2c4641e685f7a6021e7b298373febb7.
[SwitchB-pki-domain-domain2] certificate request url http://192.168.222.1:446/eadbf9af4f2c4641e685f7a6021e7b298373febb7

# Specify the CA to accept certificate requests.
[SwitchB-pki-domain-domain2] certificate request from ca

# Specify the PKI entity for certificate request as entity2.
[SwitchB-pki-domain-domain2] certificate request entity entity2

# Specify RSA key pair rsa1 with the general purpose for certificate request.
[SwitchB-pki-domain-domain2] public-key rsa general name rsa1
[SwitchB-pki-domain-domain2] quit

# Create an IKEv2 profile named profile2.
[SwitchB] ikev2 profile profile2

# Specify the local authentication method as RSA signatures.
[SwitchB-ikev2-profile-profile2] authentication-method local rsa-signature

# Specify the remote authentication method as RSA signatures.
[SwitchB-ikev2-profile-profile2] authentication-method remote rsa-signature

# Set the local identity to FQDN name www.routerb.com.
[SwitchB-ikev2-profile-profile2] identity local fqdn www.routerb.com

# Specify the peer ID that the IKEv2 profile matches. The peer ID is FQDN name www.switcha.com.
[SwitchB-ikev2-profile-profile2] match remote identity fqdn www.switcha.com
[SwitchB-ikev2-profile-profile2] quit

# Create an IKEv2 proposal named 10.
[SwitchB] ikev2 proposal 10

# Specify the integrity protection algorithm as HMAC-MD5.
[SwitchB-ikev2-proposal-10] integrity md5

# Specify the encryption algorithm as 3DES-CBC.
[SwitchB-ikev2-proposal-10] encryption 3des-cbc

# Specify the DH group as Group 1.
[SwitchB-ikev2-proposal-10] dh group1

# Specify the PRF algorithm as HMAC-MD5.
[SwitchB-ikev2-proposal-10] prf md5
[SwitchB-ikev2-proposal-10] quit

# Create an IKEv2 policy named 1.
[SwitchB] ikev2 policy 1

# Specify IKEv2 proposal 10 for the IKEv2 policy.
[SwitchB-ikev2-policy-1] proposal 10
[SwitchB-ikev2-policy-1] quit

# Create an IPsec policy template entry. Specify the template name as template1 and set the sequence number to 1.
[SwitchB] ipsec policy-template template1 1

# Specify the remote IP address 1.1.1.1 for the IPsec tunnel.
[SwitchB-ipsec-policy-template-template1-1] remote-address 1.1.1.1

# Specify ACL 3101 to identify the traffic to be protected.
[SwitchB-ipsec-policy-template-template1-1] security acl 3101

# Specify IPsec transform set tran1 for the IPsec policy template.
[SwitchB-ipsec-policy-template-template1-1] transform-set tran1

# Specify IKEv2 profile profile2 for the IPsec policy template.
[SwitchB-ipsec-policy-template-template1-1] ikev2-profile profile2
[SwitchB-ipsec-policy-template-template1-1] quit

# Create an IKE-based IPsec policy entry by using IPsec policy template template1. Specify the policy name as use1 and set the sequence number to 1.
[SwitchB] ipsec policy use1 1 isakmp template template1

# Apply IPsec policy use1 to VLAN-interface 1.
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec apply policy use1
[SwitchB-Vlan-interface1] quit

Verifying the configuration

# Initiate a connection between Switch A and Switch B to trigger IKEv2 negotiation. After IPsec SAs are successfully negotiated by IKEv2, traffic between the two switches is IPsec protected.
Troubleshooting IKEv2

IKEv2 negotiation failed because no matching IKEv2 proposals were found

Symptom
The IKEv2 SA is in IN-NEGO status.

```
<Sysname> display ikev2 sa
Tunnel ID   Local                       Remote                      Status
---------------------------------------------------------------------------
  5           123.234.234.124/500     123.234.234.123/500         IN-NEGO
```

Status:
IN-NEGO: Negotiating, EST: Establish, DEL:Deleting

Analysis
Certain IKEv2 proposal settings are incorrect.

Solution
1. Examine the IKEv2 proposal configuration to see whether the two ends have matching IKEv2 proposals.
2. Modify the IKEv2 proposal configuration to make sure the two ends have matching IKEv2 proposals.

IPsec SA negotiation failed because no matching IPsec transform sets were found

Symptom
The `display ikev2 sa` command shows that the IKEv2 SA negotiation succeeded and the IKEv2 SA is in EST status. The `display ipsec sa` command shows that the expected IPsec SAs have not been negotiated yet.

Analysis
Certain IPsec policy settings are incorrect.

Solution
1. Examine the IPsec configuration to see whether the two ends have matching IPsec transform sets.
2. Modify the IPsec configuration to make sure the two ends have matching IPsec transform sets.

IPsec tunnel establishment failed

Symptom
The ACLs and IKEv2 proposals are correctly configured on both ends. The two ends cannot establish an IPsec tunnel or cannot communicate through the established IPsec tunnel.

Analysis
The IKEv2 SA or IPsec SAs on either end are lost. The reason might be that the network is unstable and the device reboots.
Solution

1. Use the `display ikev2 sa` command to examine whether an IKEv2 SA exists on both ends. If the IKEv2 SA on one end is lost, delete the IKEv2 SA on the other end by using the `reset ikev2 sa` command and trigger new negotiation. If an IKEv2 SA exists on both ends, go to the next step.

2. Use the `display ipsec sa` command to examine whether IPsec SAs exist on both ends. If the IPsec SAs on one end are lost, delete the IPsec SAs on the other end by using the `reset ipsec sa` command and trigger new negotiation.
Configuring SSH

Overview

Secure Shell (SSH) is a network security protocol. Using encryption and authentication, SSH can implement secure remote access and file transfer over an insecure network.

SSH uses the typical client-server model to establish a channel for secure data transfer based on TCP.

SSH includes two versions: SSH1.x and SSH2.0 (hereinafter referred to as SSH1 and SSH2), which are not compatible. SSH2 is better than SSH1 in performance and security.

The device can work as an SSH server or as an SSH client.

- When acting as an SSH server, the device provides services for SSH clients and supports the following SSH versions:
  - For Secure Telnet (Stelnet), Secure File Transfer Protocol (SFTP), or Secure Copy (SCP) connections, the device supports SSH2 and SSH1 in non-FIPS mode and SSH2 in FIPS mode.
  - For NETCONF-over-SSH connections, the device supports only SSH2 in both non-FIPS and FIPS modes.
- When acting as an SSH client, the device supports only SSH2. It allows users to establish SSH connections with an SSH server.

The device supports the following SSH applications:

- **Secure Telnet**—Stelnet provides secure and reliable network terminal access services. Through Stelnet, a user can securely log in to a remote server. Stelnet can protect devices against attacks, such as IP spoofing and plain text password interception. The device can act as an Stelnet server or an Stelnet client.
- **SFTP**—Based on SSH2, it uses SSH connections to provide secure file transfer. The device can act as an SFTP server, allowing a remote user to log in to the SFTP server for secure file management and transfer. The device can also act as an SFTP client, enabling a user to log in from the device to a remote device for secure file transfer.
- **SCP**—Based on SSH2, it offers a secure approach to copying files. The device can act as an SCP server, allowing a user to log in to the device for file upload and download. The device can also act as an SCP client, enabling a user to log in from the device to a remote device for secure file transfer.
- **NETCONF over SSH**—Based on SSH2, it enables users to securely log in to the device through SSH and perform NETCONF operations on the device through the NETCONF-over-SSH connections. The device can act only as a server in NETCONF-over-SSH connections. For more information about NETCONF, see *Network Management and Monitoring Configuration Guide*.

How SSH works

This section uses SSH2 as an example to list the stages to establish an SSH session. For more information about these stages, see *SSH Technology White Paper*.

**Table 19 Stages to establish an SSH session**

<table>
<thead>
<tr>
<th>Stages</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection establishment</td>
<td>The SSH server listens to connection requests on port 22. After a client initiates a connection request, the server and the client establish a</td>
</tr>
<tr>
<td>Stages</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TCP connection</td>
<td>The two parties determine a version to use.</td>
</tr>
</tbody>
</table>
| Version negotiation    | SSH supports multiple algorithms. Based on the local algorithms, the two parties negotiate the following algorithms:  
• Key exchange algorithm for generating session keys.  
• Encryption algorithm for encrypting data.  
• Public key algorithm for digital signature and authentication.  
• HMAC algorithm for protecting data integrity. |
| Algorithm negotiation  | The two parties use the DH exchange algorithm to dynamically generate the session keys and session ID.  
• The session keys are used for protecting data transfer.  
• The session ID is used for identifying the SSH connection.  
In this stage, the client also authenticates the server. |
| Key exchange           | The SSH server authenticates the client in response to the client's authentication request. |
| Authentication         | After passing the authentication, the client sends a session request to the server to request the establishment of a session (or request the Stelnet, SFTP, SCP, or NETCONF service). |
| Session request        | After the server grants the request, the client and the server start to communicate with each other in the session.  
In this stage, you can paste commands in text format and execute them at the CLI. The text pasted at one time must be no more than 2000 bytes. As a best practice to execute the commands successfully, paste commands that are in the same view.  
To execute commands of more than 2000 bytes, save the commands in a configuration file, upload the file to the server through SFTP, and use it to restart the server. |

### SSH authentication methods

This section describes authentication methods that are supported by the device when it acts as an SSH server.

#### Password authentication

The SSH server authenticates a client through the AAA mechanism. The password authentication process is as follows:

1. The client sends the server an authentication request that includes the encrypted username and password.
2. The server performs the following operations:  
   a. Decrypts the request to get the username and password in plain text.  
   b. Verifies the username and password locally or through remote AAA authentication.  
   c. Informs the client of the authentication result.

If the AAA server requires the user to enter a password for secondary authentication, it sends the SSH server an authentication response carrying a prompt. The prompt is transparently transmitted to the client to notify the user to enter a specific password. When the user enters the correct password, the AAA server examines the password validity. If the password is valid, the SSH server returns an authentication success message to the client.

For more information about AAA, see "Configuring AAA."
NOTE:
SSH1 clients do not support secondary password authentication that is initiated by the AAA server.

Publickey authentication

The server authenticates a client by verifying the digital signature of the client. The publickey authentication process is as follows:

1. The client sends the server a publickey authentication request that includes the username, public key, and public key algorithm name.

   If the digital certificate of the client is required in authentication, the client also encapsulates the digital certificate in the authentication request. The digital certificate carries the public key information of the client.

2. The server verifies the client's public key.
   - If the public key is invalid, the server informs the client of the authentication failure.
   - If the public key is valid, the server requests the digital signature of the client. After receiving the signature, the server uses the public key to verify the signature, and informs the client of the authentication result.

When acting as an SSH server, the device supports using the public key algorithms DSA, ECDSA, and RSA to verify digital signatures.

When acting as an SSH client, the device supports using the public key algorithms DSA, ECDSA, and RSA to generate digital signatures.

For more information about public key configuration, see "Managing public keys."

Password-publickey authentication

The server requires SSH2 clients to pass both password authentication and publickey authentication. However, an SSH1 client only needs to pass either authentication, regardless of the requirement of the server.

Any authentication

The server requires clients to pass password authentication or publickey authentication.

SSH support for Suite B

Suite B contains a set of encryption and authentication algorithms that meet high security requirements. Table 20 lists all algorithms in Suite B.

The SSH server and client support using the X.509v3 certificate for identity authentication in compliance with the algorithm, negotiation, and authentication specifications defined in RFC 6239.

Table 20 Suite B algorithms

<table>
<thead>
<tr>
<th>Security level</th>
<th>Key algorithm</th>
<th>exchange algorithm</th>
<th>Encryption algorithm and HMAC algorithm</th>
<th>Public key algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>128-bit</td>
<td>ecdh-sha2-nistp256</td>
<td>AEAD_AES_128_GCM</td>
<td>x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384</td>
<td></td>
</tr>
<tr>
<td>192-bit</td>
<td>ecdh-sha2-nistp384</td>
<td>AEAD_AES_256_GCM</td>
<td>x509v3-ecdsa-sha2-nistp256</td>
<td></td>
</tr>
<tr>
<td>Both</td>
<td>ecdh-sha2-nistp256</td>
<td>AEAD_AES_128_GCM</td>
<td>x509v3-ecdsa-sha2-nistp256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdh-sha2-nistp384</td>
<td>AEAD_AES_256_GCM</td>
<td>x509v3-ecdsa-sha2-nistp384</td>
<td></td>
</tr>
</tbody>
</table>
Feature and software version compatibility

The following algorithms are available in Release 1121 and later:

- Public key algorithm ECDSA.
- Suite B algorithms.

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see "Configuring FIPS."

Configuring the device as an SSH server

You can configure the device as an Stelnet server, SFTP server, or SCP server. Because the configuration procedures are similar, the SSH server collectively refers to the Stelnet server, the SFTP server, and the SCP server unless otherwise specified.

SSH server configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Generating local key pairs</td>
<td>N/A</td>
</tr>
<tr>
<td>(Required.) Enabling the Stelnet server</td>
<td>Required for Stelnet servers.</td>
</tr>
<tr>
<td>(Required.) Enabling the SFTP server</td>
<td>Required for SFTP servers.</td>
</tr>
<tr>
<td>(Required.) Enabling the SCP server</td>
<td>Required for SCP servers.</td>
</tr>
<tr>
<td>(Required.) Configuring NETCONF over SSH</td>
<td>Required for NETCONF-over-SSH servers.</td>
</tr>
<tr>
<td>(Required.) Configuring user lines for SSH login</td>
<td>Required for Stelnet servers and NETCONF-over-SSH servers.</td>
</tr>
<tr>
<td>(Required.) Configuring a client's host public key</td>
<td>Required if the authentication method is publickey, password-publickey, or any.</td>
</tr>
</tbody>
</table>
| Configuring the PKI domain for verifying the client certificate | See "Configuring PKI."
  Required if the following conditions exist:
  - The authentication method is publickey.
  - The clients send the public keys to the server through digital certificates for validity check.
  The PKI domain must have the CA certificate to verify the client certificate. |
| (Required/optional.) Configuring an SSH user | Required if the authentication method is publickey, password-publickey, or any. Optional if the authentication method is password. |
| (Optional.) Configuring the SSH management parameters | N/A                                           |
| (Optional.) Specifying a PKI domain for the SSH server | N/A                                           |
Generating local key pairs

The DSA, ECDSA, or RSA key pairs are required for generating the session keys and session ID in the key exchange stage. They can also be used by a client to authenticate the server. When a client authenticates the server, it compares the public key received from the server with the server's public key that the client saved locally. If the keys are consistent, the client uses the locally saved server's public key to decrypt the digital signature received from the server. If the decryption succeeds, the server passes the authentication.

When you execute any one of the SSH commands on the device to trigger the running of the SSH application, the SSH server automatically generates two RSA key pairs. You can also use the `public-key local create` command to generate DSA, ECDSA, or RSA key pairs on the device.

Configuration guidelines

When you use the `public-key local create` command to generate local key pairs, follow these restrictions and guidelines:

- Local DSA, ECDSA, and RSA key pairs for SSH use default names. You cannot assign names to the key pairs.
- To support SSH clients that use different types of key pairs, generate DSA, ECDSA, and RSA key pairs on the SSH server.
- The SSH server operating in FIPS mode supports only ECDSA and RSA key pairs. If both ECDSA and RSA key pairs exist on the server, the server uses the ECDSA key pair.
- The `public-key local create rsa` command generates a server key pair and a host key pair for RSA. In SSH1, the public key in the server key pair is used to encrypt the session key for secure transmission of the session key. Because SSH2 uses the DH algorithm to generate each session key on the SSH server and the client, no session key transmission is required. The server key pair is not used in SSH2.
- The `public-key local create dsa` command generates only a DSA host key pair. SSH1 does not support the DSA algorithm.
- The key modulus length must be less than 2048 bits when you use the `public-key local create dsa` command on the SSH server.
- The `public-key local create ecdsa` command generates only an ECDSA host key pair. SSH1 does not support the ECDSA algorithm.

Configuration procedure

To generate local key pairs on the SSH server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | Generate local key pairs. | [In Release 1111: public-key local create { dsa | rsa }](#)  
|      |          |         |
|      | In Release 1121 and later: public-key local create { dsa | ecdsa { secp256r1 | secp384r1 } | rsa } | By default, no local key pairs exist. |

Enabling the Stelnet server

After you enable the Stelnet server on the device, a client can log in to the device through Stelnet.

To enable the Stelnet server:
### Enabling the SFTP server

After you enable the SFTP server on the device, a client can log in to the device through SFTP.

To enable the SFTP server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable the SFTP server.</td>
<td>sftp server enable</td>
<td>By default, the SFTP server is disabled.</td>
</tr>
</tbody>
</table>

### Enabling the SCP server

After you enable the SCP server on the device, a client can log in to the device through SCP.

The device that acts as an SCP server does not support SCP connections initiated by SSH1 clients.

To enable the SCP server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable the SCP server.</td>
<td>scp server enable</td>
<td>By default, the SCP server is disabled.</td>
</tr>
</tbody>
</table>

### Configuring NETCONF over SSH

After you enable NETCONF over SSH on the device, a client can perform NETCONF operations on the device through a NETCONF-over-SSH connection.

When the device acts as a server in the NETCONF-over-SSH connection, connection requests initiated by SSH1 clients are not supported.

For more information about NETCONF over SSH commands, see *Network Management and Monitoring Command Reference*.

To configure NETCONF over SSH:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable NETCONF over SSH.</td>
<td>netconf ssh server enable</td>
<td>By default, NETCONF over SSH is disabled.</td>
</tr>
<tr>
<td>3. Specify a port to listen for NETCONF-over-SSH connections.</td>
<td>netconf ssh server port port-number</td>
<td>By default, port 830 listens for NETCONF-over-SSH connections.</td>
</tr>
</tbody>
</table>
Configuring user lines for SSH login

Depending on the SSH application, an SSH client can be an Stelnet client, SFTP client, SCP client, or NETCONF-over-SSH client.

Only Stelnet and NETCONF-over-SSH clients require the user line configuration. The user line configuration takes effect on the clients at the next login.

To configure the user lines for Stelnet and NETCONF-over-SSH clients:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VTY user line view.</td>
<td>line vty number [ending-number]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the login authentication mode to scheme.</td>
<td>authentication-mode scheme</td>
</tr>
</tbody>
</table>

Configuring a client's host public key

In publickey authentication, the server compares the SSH username and client's host public key that it receives from the client with the locally saved SSH username and the client's host public key. If they are the same, the server checks the digital signature that the client sends. The client generates the digital signature by using the private key that is associated with the client's host public key.

For publickey authentication, password-publickey authentication, or any authentication, you must perform the following tasks:

1. Configure the client's DSA, ECDSA, or RSA host public key on the server.
   - As a best practice, configure no more than 20 SSH client host public keys on an SSH server.
2. Specify the associated host private key on the client to generate the digital signature.
   - If the device acts as an SSH client, specify the public key algorithm on the client. The algorithm determines the associated host private key for generating the digital signature.

You can enter the content of a client's host public key or import the client's host public key from the public key file. As a best practice, import the client's host public key.

Entering a client's host public key

Before you enter the client's host public key, you must use the display public-key local public command on the client to obtain the client's host public key.

To enter a client's host public key:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter public key view.</td>
<td>public-key peer keyname</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a client's host public key.</td>
<td>Enter the content of the host public key</td>
</tr>
</tbody>
</table>
Importing the client’s host public key from the public key file

Before you import the host public key, upload the client's public key file (in binary) to the server, for example, through FTP or TFTP. During the import process, the server automatically converts the host public key in the public key file to a string in PKCS format.

To import a client's host public key from the public key file:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Import a client's public key from a public key file.</td>
<td>public-key peer keyname import sshkey filename</td>
</tr>
</tbody>
</table>

Configuring an SSH user

Configure an SSH user and a local user depending on the authentication method.

- If the authentication method is **publickey**, you must create an SSH user and a local user on the SSH server. The two users must have the same username, so that the SSH user can be assigned the correct working directory and user role.

- If the authentication method is **password**, you must perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

You do not need to create an SSH user by using the `ssh user` command. However, if you want to display all SSH users, including the password-only SSH users, for centralized management, you can use this command to create them. If such an SSH user has been created, make sure you have specified the correct service type and authentication method.

- If the authentication method is **password-publickey** or **any**, you must create an SSH user and perform one of the following tasks:
  - For local authentication, configure a local user on the SSH server.
  - For remote authentication, configure an SSH user on a remote authentication server, for example, a RADIUS server.

In either case, the local user or the SSH user configured on the remote authentication server must have the same username as the SSH user.

Configuration guidelines

When you configure an SSH user, follow these restrictions and guidelines:

- An SSH server supports up to 1024 SSH users.
- For an SFTP or SCP user, the working directory depends on the authentication method.
  - If the authentication method is **password**, the working directory is authorized by AAA.
  - If the authentication method is **publickey** or **password-publickey**, the working folder is specified by the `authorization-attribute` command in the associated local user view.
- For an SSH user, the user role also depends on the authentication method.
If the authentication method is password, the user role is authorized by the remote AAA server or the local device.

If the authentication method is publickey or password-publickey, the user role is specified by the authorization-attribute command in the associated local user view.

- If you change the authentication method or public key for a logged-in SSH user, the changes take effect at the next login.
- For all authentication methods except password authentication, you must specify a client's host public key or digital certificate.
  - For a client that directly sends the user's public key information to the server, you must specify the client's host public key on the server. The specified public key must already exist. For more information about public keys, see "Configuring a client's host public key."
  - For a client that sends the user's public key information to the server through a digital certificate, you must specify the PKI domain on the server. This PKI domain verifies the client certificate. To make sure the authorized SSH users can pass the authentication, the specified PKI domain must have the correct CA certificate. To specify the PKI domain, use the ssh user or ssh server pki-domain command. For more information about configuring a PKI domain, see "Configuring PKI."

- When the device operates in FIPS mode as an SSH server, the device does not support the authentication method of any or publickey.

For information about configuring local users and remote authentication, see "Configuring AAA."

**Configuration procedure**

To configure an SSH user, and specify the service type and authentication method:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
</tr>
</tbody>
</table>

2. Create an SSH user, and specify the service type and authentication method.

   - In Release 1111:
     - In non-FIPS mode: ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type { password | { any | password-publickey | publickey } assign { pki-domain domain-name | publickey keyname } }
     - In FIPS mode: ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type { password | password-publickey assign { pki-domain domain-name | publickey keyname } }

   - In Release 1121 and later:
     - In non-FIPS mode: ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type { password | { any | password-publickey | publickey } assign { pki-domain domain-name | publickey keyname } }
     - In FIPS mode: ssh user username service-type { all | netconf | scp | sftp | stelnet } authentication-type { password | password-publickey [ assign { pki-domain domain-name | publickey keyname } ] }

**Configuring the SSH management parameters**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>2. Enable the SSH server to support SSH1 clients.</td>
<td><code>ssh server compatible-ssh1x enable</code></td>
<td>By default, the SSH server supports SSH1 clients. This command is not available in FIPS mode.</td>
</tr>
<tr>
<td>3. Set the RSA server key pair update interval.</td>
<td><code>ssh server rekey-interval hours</code></td>
<td>By default, the device does not update the RSA server key pair. This command takes effect only on SSH1 users. This command is not available in FIPS mode.</td>
</tr>
<tr>
<td>4. Set the SSH user authentication timeout timer.</td>
<td><code>ssh server authentication-timeout time-out-value</code></td>
<td>The default setting is 60 seconds. If a user does not finish the authentication when the timeout timer expires, the connection cannot be established.</td>
</tr>
<tr>
<td>5. Set the maximum number of SSH authentication attempts.</td>
<td><code>ssh server authentication-retries times</code></td>
<td>The default setting is 3. If a user does not finish the authentication when the timeout timer expires, the connection cannot be established.</td>
</tr>
<tr>
<td>6. Specify an ACL to control SSH user connections.</td>
<td>- Control IPv4 SSH user connections: <code>ssh server acl acl-number</code> - Control IPv6 SSH user connections: <code>ssh server ipv6 acl [ ipv6 ] acl-number</code></td>
<td>By default, no ACLs are specified and all SSH users can initiate connections to the server.</td>
</tr>
<tr>
<td>7. Set the DSCP value in the packets that the SSH server sends to the SSH clients.</td>
<td>- Set the DSCP value in IPv4 packets: <code>ssh server dscp dscp-value</code> - Set the DSCP value in IPv6 packets: <code>ssh server ipv6 dscp dscp-value</code></td>
<td>The default setting is 48. The DSCP value of a packet defines the priority of the packet and affects the transmission priority of the packet. A bigger DSCP value represents a higher priority.</td>
</tr>
<tr>
<td>8. Configure the SFTP connection idle timeout timer.</td>
<td><code>sftp server idle-timeout time-out-value</code></td>
<td>The default setting is 10 minutes. When the idle timeout timer expires, the system automatically terminates the connection.</td>
</tr>
<tr>
<td>9. Specify the maximum number of concurrent online SSH users.</td>
<td><code>aaa session-limit ssh max-sessions</code></td>
<td>The default setting is 32. When the number of online SSH users reaches the upper limit, the system denies new SSH connection requests. Changing the upper limit does not affect online SSH users.</td>
</tr>
</tbody>
</table>

**Specifying a PKI domain for the SSH server**

**IMPORTANT:**
This feature is available in Release 1121 and later.
The PKI domain specified for the SSH server has the following functions:

- The SSH server uses the PKI domain to send its certificate to the client in the key exchange stage.
- The SSH server uses the PKI domain to authenticate the client’s certificate if no PKI domain is specified for the client authentication by using the `ssh user` command.

To specify a PKI domain for the SSH server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify a PKI domain for the SSH server.</td>
<td>ssh server pki-domain domain-name</td>
</tr>
</tbody>
</table>

Configuring the device as an Stelnet client

Stelnet client configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Specifying the source IP address for SSH packets</td>
</tr>
<tr>
<td>(Required.) Establishing a connection to an Stelnet server</td>
</tr>
<tr>
<td>(Optional.) Establishing a connection to an Stelnet server based on Suite B</td>
</tr>
</tbody>
</table>

Specifying the source IP address for SSH packets

As a best practice, specify the IP address of the loopback interface as the source interface for SSH packets for the following purposes:

- Ensuring the communication between the Stelnet client and the Stelnet server.
- Improving the manageability of Stelnet clients in authentication service.

To specify the source IP address for SSH packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Specify the source address for SSH packets. | ```
Specify the source IPv4 address for SSH packets:

```
ssh client source { interface interface-type interface-number | ip ip-address }
```

Specify the source IPv6 address for SSH packets:

```
ssh client ipv6 source { interface interface-type interface-number | ipv6 ipv6-address }
```

By default, the source IP address for SSH packets is not configured. For IPv4 SSH packets, the device uses the primary IPv4 address of the output interface specified in the routing entry as the source address of the packets. For IPv6 SSH packets, the device automatically selects an IPv6 address as the source address of the packets in compliance with RFC 3484. |
Establishing a connection to an Stelnet server

When you try to access an Stelnet server, the device must use the server’s host public key to authenticate the server. If the server's host public key is not configured on the device, the device will notify you to confirm whether to continue with the access.

- If you choose to continue, the device accesses the server and downloads the server's host public key.
- If you choose to not continue, the connection cannot be established.

As a best practice, configure the server’s host public key on the device in an insecure network.

To establish a connection to an Stelnet server in Release 1111:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Establish a connection to an Stelnet server. | In non-FIPS mode, establish a connection to an IPv4 Stelnet server: 

```bash
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | rsa } ]
prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | 
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | aes256 | des } | 
prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } | * [ dscp dscp-value | escape character | publickey keyname | source { interface interface-type interface-number | ip ip-address } ] |
```

- In FIPS mode, establish a connection to an IPv4 Stelnet server: 

```bash
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key rsa ]
prefer-compress zlib | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | 
prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } | * [ escape character | publickey keyname | source { interface interface-type interface-number | ip ip-address } ] |
```

- In non-FIPS mode, establish a connection to an IPv6 Stelnet server: 

```bash
ssh2 ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | rsa } ]
prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | 
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex dh-group-exchange | 
prefer-stoc-cipher { 3des | aes128 | aes256 | des } | 
prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } | * [ dscp dscp-value | escape character | publickey keyname | source { interface interface-type interface-number | ip ip-address } ] |
```

- In FIPS mode, establish a connection to an IPv6 Stelnet server: 

```bash
ssh2 ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ identity-key rsa ]
```
To establish a connection to an Stelnet server in Release 1121 and later:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a connection to an Stelnet server.</td>
<td>`interface-number</td>
<td>identity-key rsa</td>
</tr>
<tr>
<td>Task</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remarks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>domain-name</td>
<td>prefer-compress zlib</td>
<td></td>
</tr>
<tr>
<td>• In non-FIPS mode, establish a connection to an IPv6 Stelnet server: ssh2 ipv6 server [ port-number</td>
<td>] [ vpn-instance vpn-instance-name</td>
<td>] [ -i interface-type</td>
</tr>
<tr>
<td>• In FIPS mode, establish a connection to an IPv6 Stelnet server: ssh2 ipv6 server [ port-number</td>
<td>] [ vpn-instance vpn-instance-name</td>
<td>] [ -i interface-type</td>
</tr>
</tbody>
</table>
Establishing a connection to an Stelnet server based on Suite B

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a connection to an IPv4 Stelnet server based on Suite B.</td>
<td>`ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] suite-b [ 128-bit</td>
<td>192-bit ] pki-domain domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ dscp dscp-value</td>
</tr>
<tr>
<td>Establish a connection to an IPv6 Stelnet server based on Suite B.</td>
<td>`ssh2 ipv6 server [ port-number ] [ i interface-type interface-number ] [ vpn-instance vpn-instance-name ] suite-b [ 128-bit</td>
<td>192-bit ] pki-domain domain-name [ server-pki-domain domain-name ] [ interface interface-type interface-number ] [ prefer-compress zlib ] [ dscp dscp-value</td>
</tr>
</tbody>
</table>

Configuring the device as an SFTP client

SFTP client configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Specifying the source IP address for SFTP packets</td>
</tr>
<tr>
<td>(Required.) Establishing a connection to an SFTP server</td>
</tr>
<tr>
<td>(Optional.) Establishing a connection to an SFTP server based on Suite B</td>
</tr>
<tr>
<td>(Optional.) Working with SFTP directories</td>
</tr>
<tr>
<td>(Optional.) Working with SFTP files</td>
</tr>
<tr>
<td>(Optional.) Displaying help information</td>
</tr>
<tr>
<td>(Optional.) Terminating the connection with the SFTP server</td>
</tr>
</tbody>
</table>

Specifying the source IP address for SFTP packets

As a best practice, specify the IP address of the loopback interface as the source interface for SFTP packets for the following purposes:

- Ensuring the communication between the SFTP client and the SFTP server.
- Improving the manageability of SFTP clients in the authentication service.
To specify the source IP address for SFTP packets:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Specify the source address for SFTP packets. | • Specify the source IPv4 address for SFTP packets: `sftp client source { ip ip-address | interface interface-type interface-number }`
• Specify the source IPv6 address for SFTP packets: `sftp client ipv6 source { ipv6 ipv6-address | interface interface-type interface-number }` | By default, the source IP address for SFTP packets is not configured. For IPv4 SFTP packets, the device uses the primary IPv4 address of the output interface specified in the routing entry as the source address of the packets. For IPv6 SFTP packets, the device automatically selects an IPv6 address as the source address of the packets in compliance with RFC 3484. |

**Establishing a connection to an SFTP server**

When you try to access an SFTP server, the device must use the server's host public key to authenticate the server. If the server's host public key is not configured on the device, the device will notify you to confirm whether to continue with the access.

- If you choose to continue, the device accesses the server and downloads the server's host public key.
- If you choose to not continue, the connection cannot be established.

As a best practice, configure the server's host public key on the device in an insecure network.

After the connection is established, you can directly enter SFTP client view on the server to perform file or directory operations.

To establish a connection to an SFTP server in Release 1111:
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Establish a connection to an SFTP server. | In non-FIPS mode, establish a connection to an IPv4 SFTP server:  
`sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 | prefer-stoc-cipher { 3des | aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } } [ dscp dscp-value | publickey keyname | source { interface interface-type interface-number | ip ip-address }] ] *` | Available in user view. |
| | In FIPS mode, establish a connection to an IPv4 SFTP server:  
`sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key rsa | prefer-compress zlib | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } } [ publickey keyname | source { interface interface-type interface-number | ip ip-address }] ] *` | |
| | In non-FIPS mode, establish a connection to an IPv6 SFTP server:  
`sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ identity-key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { 3des | aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } } [ dscp dscp-value | publickey keyname | source { interface interface-type interface-number | ipv6 ipv6-address }] ] *` | |
| | In FIPS mode, establish a connection to an IPv6 SFTP server:  
`sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ identity-key rsa | prefer-compress zlib | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } } [ publickey keyname | source { interface interface-type interface-number | ipv6 ipv6-address }] ] *` | |

To establish a connection to an SFTP server in Release 1121 and later:
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• In FIPS mode, establish a connection to an IPv4 SFTP server:</td>
<td>`sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { ecdsa</td>
<td>rsa</td>
</tr>
<tr>
<td>• In non-FIPS mode, establish a connection to an IPv6 SFTP server:</td>
<td>`sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ identity-key { dsa</td>
<td>ecdsa</td>
</tr>
</tbody>
</table>
Establishing a connection to an SFTP server based on Suite B

After the connection is established, you are in SFTP client view of the server and can perform file or directory operations.

To establish a connection to an SFTP server based on Suite B:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a connection to an IPv4 SFTP server based on Suite B.</td>
<td>`sftp server [ port-number ] [ vpn-instance vpn-instance-name ] suite-b [128-bit</td>
<td>Available in user view. The client cannot establish connections to both IPv4 and IPv6 SFTP servers.</td>
</tr>
</tbody>
</table>
## Working with SFTP directories

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the working directory on the SFTP server.</td>
<td>cd [remote-path]</td>
<td>Available in SFTP client view.</td>
</tr>
<tr>
<td>Return to the upper-level directory.</td>
<td>cdup</td>
<td>Available in SFTP client view.</td>
</tr>
<tr>
<td>Display the current working directory on the SFTP server.</td>
<td>pwd</td>
<td>Available in SFTP client view.</td>
</tr>
<tr>
<td>Display files under a directory.</td>
<td>dir [-a</td>
<td>-l] [remote-path]</td>
</tr>
<tr>
<td></td>
<td>ls [-a</td>
<td>-l] [remote-path]</td>
</tr>
<tr>
<td>Change the name of a directory on the SFTP server.</td>
<td>rename oldname newname</td>
<td>Available in SFTP client view.</td>
</tr>
<tr>
<td>Create a new directory on the SFTP server.</td>
<td>mkdir remote-path</td>
<td>Available in SFTP client view.</td>
</tr>
<tr>
<td>Delete one or more directories from the SFTP server.</td>
<td>rmdir remote-path</td>
<td>Available in SFTP client view.</td>
</tr>
</tbody>
</table>

## Working with SFTP files

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the name of a file on the SFTP server.</td>
<td>rename old-name new-name</td>
<td>Available in SFTP client view.</td>
</tr>
<tr>
<td>Download a file from the remote server and save it locally.</td>
<td>get remote-file [local-file]</td>
<td>Available in SFTP client view.</td>
</tr>
<tr>
<td>Display the files under a directory.</td>
<td>dir [-a</td>
<td>-l] [remote-path]</td>
</tr>
<tr>
<td></td>
<td>ls [-a</td>
<td>-l] [remote-path]</td>
</tr>
<tr>
<td>Delete one or more directories from the SFTP server.</td>
<td>delete remote-file</td>
<td>Available in SFTP client view. The delete command has the same function as the remove command.</td>
</tr>
<tr>
<td></td>
<td>remove remote-file</td>
<td></td>
</tr>
</tbody>
</table>

## Displaying help information

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the help information of SFTP client commands.</td>
<td>help</td>
<td>Available in SFTP client view.</td>
</tr>
<tr>
<td></td>
<td>?</td>
<td></td>
</tr>
</tbody>
</table>
**Terminating the connection with the SFTP server**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Terminate the connection with the SFTP server and return to user view. | • bye  
• exit  
• quit | Available in SFTP client view. These three commands have the same function. |

**Configuring the device as an SCP client**

This section describes how to configure the device as an SCP client to establish a connection with an SCP server and transfer files with the server.

**Establishing a connection to an SCP server**

When you try to access an SCP server, the device must use the server's host public key to authenticate the server. If the server's host public key is not configured on the device, the device will notify you to confirm whether to continue with the access.

- If you choose to continue, the device accesses the server and downloads the server's host public key.
- If you choose to not continue, the connection cannot be established.

As a best practice, configure the server's host public key on the device in an insecure network.

To transfer files with an SCP server in Release 1111:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Connect to the SCP server, and transfer files with the server. | • In non-FIPS mode, connect to the IPv4 SCP server, and transfer files with this server:  
```  
scp server [ port-number ] [ vpn-instance vpn-instance-name ] | { put | get } source-file-name [ destination-file-name ] | { identity-key { dsa | rsa } | prefer-compress zlib | prefer-ctos-cipher { 3des | aes128 | aes256 | des } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 } | prefer-kex { dh-group-exchange | dh-group1 | dh-group14 } | prefer-stoc-cipher { 3des | aes128 | aes256 | des } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 } } * | publickey keyname | source { interface interface-type interface-number | ip ip-address } } *  
```  
| • In FIPS mode, connect to the IPv4 SCP server, and transfer files with this server:  
```  
scp server [ port-number ] [ vpn-instance vpn-instance-name ] | { put | get } source-file-name [ destination-file-name ] | { identity-key rsa | prefer-compress zlib | prefer-ctos-cipher { aes128 | aes256 } | prefer-ctos-hmac { sha1 | sha1-96 } | prefer-kex dh-group14 | prefer-stoc-cipher { aes128 | aes256 } | prefer-stoc-hmac { sha1 | sha1-96 } } * | publickey keyname | source { interface interface-type interface-number | ip ip-address } } *  
```  
| Available in user view. |
To transfer files with an SCP server in Release 1121 and later:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• In non-FIPS mode, connect to the IPv4 SCP server, and transfer files with this server: `scp server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] { put</td>
<td>get } source-file-name [ destination-file-name ] [ identity-key { dsa</td>
<td>rsa } ] [ prefer-compress zlib</td>
</tr>
<tr>
<td>• In FIPS mode, connect to the IPv4 SCP server, and transfer files with this server: `scp server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] { put</td>
<td>get } source-file-name [ destination-file-name ] [ identity-key rsa</td>
<td>prefer-compress zlib</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>• In non-FIPS mode, connect to the IPv6 SCP server, and transfer files with this server: `scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] { put</td>
<td>get } source-file-name [ destination-file-name ] [ identity-key { dsa</td>
<td>rsa } ] [ prefer-compress zlib</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>vpn-instance-name</strong> [ put</td>
<td>get ] source-file-name [ destination-file-name ] [ identity-key { ecdsa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>In non-FIPS mode, connect to the IPv6 SCP server, and transfer files with this server: sudo scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ put</td>
<td>get ] source-file-name [ destination-file-name ] [ identity-key { dsa</td>
</tr>
<tr>
<td>•</td>
<td>In FIPS mode, connect to the IPv6 SCP server, and transfer files with this server: sudo scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] [ put</td>
<td>get ] source-file-name [ destination-file-name ] [ identity-key { ecdsa</td>
</tr>
</tbody>
</table>
### Establishing a connection to an SCP server based on Suite B

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a connection to an SCP server based on Suite B.</td>
<td></td>
<td>Available in user view. The client cannot establish connections to both IPv4 and IPv6 SCP servers.</td>
</tr>
</tbody>
</table>

- Establish a connection to an IPv4 SCP server based on Suite B: `scp server [ port-number ] [ vpn-instance vpn-instance-name ] { put | get } source-file-name [ destination-file-name ] suite-b [ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ source { interface interface-type interface-number | ipv6 ipv6-address } ] *` |

- Establish a connection to an IPv6 SCP server based on Suite B: `scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i interface-type interface-number ] { put | get } source-file-name [ destination-file-name ] suite-b [ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ source { interface interface-type interface-number | ipv6 ipv6-address } ] *` |

### Specifying algorithms for SSH2

**IMPORTANT:**
This feature is available in Release 1121 and later.

Perform this task to specify the following types of algorithms that the SSH2 client and server use for algorithm negotiation during the Stelnet, SFTP, or SCP session establishment:

- Key exchange algorithms.
- Public key algorithms.
- Encryption algorithms.
- MAC algorithms.
If you specify algorithms, SSH2 uses only the specified algorithms for algorithm negotiation. The client uses the specified algorithms to initiate the negotiation, and the server uses the matching algorithms to negotiate with the client.

If multiple algorithms of the same type are specified, the algorithm specified earlier has a higher priority during negotiation. The specified SSH2 algorithms do not affect SSH1 sessions.

### Specifying key exchange algorithms for SSH2

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify key exchange algorithms for SSH2.</td>
<td>• In non-FIPS mode: ssh2 algorithm key-exchange { dh-group-exchange-sha1</td>
</tr>
</tbody>
</table>

### Specifying public key algorithms for SSH2

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify public key algorithms for SSH2.</td>
<td>• In non-FIPS mode: ssh2 algorithm public-key { dsa</td>
</tr>
</tbody>
</table>

### Specifying encryption algorithms for SSH2

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Specify encryption algorithms for SSH2.</td>
<td>• In non-FIPS mode: ssh2 algorithm cipher { des-cbc</td>
</tr>
</tbody>
</table>
Specifying MAC algorithms for SSH2

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>

By default, SSH2 uses the MAC algorithms sha2-256, sha2-512, sha1, md5, sha1-96, and md5-96 in descending order of priority for algorithm negotiation.

Displaying and maintaining SSH

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the source IP address configured for the SFTP client.</td>
<td><code>display sftp client source</code></td>
</tr>
<tr>
<td>Display the source IP address configured for the Stelnet client.</td>
<td><code>display ssh client source</code></td>
</tr>
<tr>
<td>Display SSH server status or sessions.</td>
<td>`display ssh server { session</td>
</tr>
<tr>
<td>Display SSH user information on the SSH server.</td>
<td><code>display ssh user-information [ username ]</code></td>
</tr>
<tr>
<td>Display the public keys of the local key pairs.</td>
<td>`display public-key local { dsa</td>
</tr>
<tr>
<td>Display the public keys of the SSH peers.</td>
<td>`display public-key peer { brief</td>
</tr>
</tbody>
</table>

Stelnet configuration examples

Devices in the configuration examples are in non-FIPS mode.

When you configure Stelnet on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of RSA key pairs must be 2048 bits.
- When the device acts as the Stelnet server, it supports only ECDSA and RSA key pairs. If both ECDSA and RSA key pairs exist on the server, the server uses the ECDSA key pair.
Password authentication enabled Stelnet server configuration example

Network requirements

As shown in Figure 95:

- You can log in to Switch through the Stelnet client that runs on the host.
- After login, you are assigned the user role network-admin for configuration management.
- The switch acts as the Stelnet server and uses password authentication.
- The username and password of the client are saved on the switch.

**Figure 95 Network diagram**

Configuration procedure

1. **Configure the Stelnet server:**
   
   # Generate RSA key pairs.
   
   `<Switch>` system-view
   
   `[Switch]` public-key local create rsa
   
   The range of public key size is (512 ~ 2048).
   
   If the key modulus is greater than 512, it will take a few minutes.
   
   Press CTRL+C to abort.
   
   Input the modulus length [default = 1024]:
   
   Generating Keys...
   
   ........................................+++++
   
   ........................................+++++
   
   ................................................................+
   
   Create the key pair successfully.
   
   # Generate a DSA key pair.
   
   `[Switch]` public-key local create dsa
   
   The range of public key size is (512 ~ 2048).
   
   If the key modulus is greater than 512, it will take a few minutes.
   
   Press CTRL+C to abort.
   
   Input the modulus length [default = 1024]:
   
   Generating Keys...
   
   ........................................+++++
   
   ........................................+++++
   
   ................................................................+
   
   Create the key pair successfully.
   
   # Generate an ECDSA key pair.
   
   `[Switch]` public-key local create ecdsa secp256r1
   
   Generating Keys...
   
   .
Create the key pair successfully.

# Enable the Stelnet server.
[Switch] ssh server enable

# Assign an IP address to VLAN-interface 2. The Stelnet client uses this IP address as the destination for SSH connection.
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit

# Set the authentication mode to AAA for the user lines.
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit

# Create a local device management user client001.
[Switch] local-user client001 class manage

# Specify the plaintext password as aabbcc and the service type as ssh for the user.
[Switch-luser-manage-client001] password simple aabbcc
[Switch-luser-manage-client001] service-type ssh

# Assign the user role network-admin to the user.
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit

# Create an SSH user client001. Specify the service type as stelnet and the authentication method as password for the user.
[Switch] ssh user client001 service-type stelnet authentication-type password

2. Establish a connection to the Stelnet server:

   There are different types of Stelnet client software, such as PuTTY and OpenSSH. This example uses an Stelnet client that runs PuTTY version 0.58.

   To establish a connection to the Stelnet server:
   a. Launch PuTTY.exe to enter the interface shown in Figure 96.
   b. In the Host Name (or IP address) field, enter the IP address 192.168.1.40 of the Stelnet server.
c. Click **Open** to connect to the server.

If the connection is successfully established, the system notifies you to enter the username and password. After entering the username (**client001** in this example) and password (**aabbcc** in this example), you can enter the CLI of the server.

**Publickey authentication enabled Stelnet server configuration example**

**Network requirements**

As shown in **Figure 97**:

- You can log in to the switch through the Stelnet client (SSH2) that runs on the host.
- After login, you are assigned the user role network-admin for configuration management.
- The switch acts as the Stelnet server and uses publickey authentication and the RSA public key algorithm.
Configuration procedure

In the server configuration, the client's host public key is required. Use the client software to generate RSA key pairs on the client before configuring the Steinet server.

There are different types of Steinet client software, such as PuTTY and OpenSSH. This example uses an Steinet client that runs PuTTY version 0.58.

The configuration procedure is as follows:

1. Generate RSA key pairs on the Steinet client:
   a. Run PuTTYGen.exe on the client, select SSH-2 RSA and click Generate.

   Figure 98 Generating a key pair on the client

   ![PuTTY Key Generator](image)

   a. Continue moving the mouse during the key generating process, but do not place the mouse over the green progress bar shown in Figure 99. Otherwise, the progress bar stops moving and the key pair generating progress stops.
c. After the key pair is generated, click **Save public key** to save the public key. A file saving window appears.

d. Enter a file name (**key.pub** in this example), and click **Save**.

Figure 100 Saving a key pair on the client
e. On the page as shown in Figure 100, click **Save private key** to save the private key. A confirmation dialog box appears.

f. Click **Yes**. A file saving window appears.

g. Enter a file name (**private.ppk** in this example), and click **Save**.

h. Transmit the public key file to the server through FTP or TFTP. (Details not shown.)

2. Configure the Stelnet server:

   # Generate RSA key pairs.
   ```
   <Switch> system-view
   [Switch] public-key local create rsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   ........................................+++++
   .....................+++++
   .........................+++++
   Create the key pair successfully.
   ```

   # Generate a DSA key pair.
   ```
   [Switch] public-key local create dsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   ........................................+++++
   .....................+++++
   .........................+++++
   Create the key pair successfully.
   ```

   # Generate an ECDSA key pair.
   ```
   [Switch] public-key local create ecdsa secp256r1
   Generating Keys...
   Create the key pair successfully.
   ```

   # Enable the Stelnet server.
   ```
   [Switch] ssh server enable
   ```

   # Assign an IP address to VLAN-interface 2. The Stelnet client uses this IP address as the destination for SSH connection.
   ```
   [Switch] interface vlan-interface 2
   [Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
   [Switch-Vlan-interface2] quit
   ```

   # Set the authentication mode to AAA for the user lines.
   ```
   [Switch] line vty 0 63
   ```
# Import the client's public key from file key.pub and name it switchkey.

[Switch] public-key peer switchkey import sshkey key.pub

# Create an SSH user client002. Specify the authentication method as publickey for the user. Assign the public key switchkey to the user.

[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey switchkey

# Create a local device management user client002. Specify the service type as ssh for the user. Assign the user role network-admin to the user.

[Switch] local-user client002 class manage
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit

3. Specify the private key file and establish a connection to the Stelnet server:
   a. Launch PuTTY.exe on the Stelnet client to enter the interface shown in Figure 101.
   b. In the Host Name (or IP address) field, enter the IP address **192.168.1.40** of the Stelnet server.

   ![Figure 101 Specifying the host name (or IP address)](image)

   c. Select Connection > SSH from the navigation tree.
      The window shown in Figure 102 appears.
   d. Specify the **Preferred SSH protocol version** as **2** in the Protocol options area.
e. Select **Connection > SSH > Auth** from the navigation tree.

The window shown in Figure 103 appears.

f. Click **Browse...** to bring up the file selection window, navigate to the private key file (`private.ppk` in this example), and click **OK**.

**Figure 103 Specifying the private key file**
g. Click Open to connect to the server.
If the connection is successfully established, the system notifies you to enter the username.
After entering the username (client002), you can enter the CLI of the server.

**Password authentication enabled Stelnet client configuration example**

**Network requirements**
As shown in Figure 104:
- You can log in to Switch B through the Stelnet client that runs on Switch A.
- After login, you are assigned the user role network-admin for configuration management.
- Switch B acts as the Stelnet server and uses password authentication.
- The username and password of the client are saved on Switch B.

**Figure 104 Network diagram**

**Configuration procedure**
1. Configure the Stelnet server:
   # Generate RSA key pairs.
   ```
   <SwitchB> system-view
   [SwitchB] public-key local create rsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   ............................................+++++
   ............................................+++++
   ............................................+++++
   ............................................+++++
   Create the key pair successfully.
   ```
   # Generate a DSA key pair.
   ```
   [SwitchB] public-key local create dsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   ............................................+++++
   ............................................+++++
   ............................................+++++
   ............................................+++++
   ............................................+++++
   ............................................+++++
   ............................................+++++
   ............................................+++++
   Create the key pair successfully.
   ```
# Generate an ECDSA key pair.
[SwitchB] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.

# Enable the Stelnet server.
[SwitchB] ssh server enable

# Assign an IP address to VLAN-interface 2. The Stelnet client uses the address as the destination address of the SSH connection.
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[SwitchB-Vlan-interface2] quit

# Set the authentication mode to AAA for the user lines.
[SwitchB] line vty 0 63
[SwitchB-line-vty0-63] authentication-mode scheme
[SwitchB-line-vty0-63] quit

# Create a local device management user client001.
[SwitchB] local-user client001 class manage
# Specify the plaintext password as aabbcc and the service type as ssh for the user.
[SwitchB-luser-manage-client001] password simple aabbcc
[SwitchB-luser-manage-client001] service-type ssh
# Assign the user role network-admin to the user.
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit

# Create an SSH user client001. Specify the service type as stelnet and the authentication method as password for the user.
[SwitchB] ssh user client001 service-type stelnet authentication-type password

2. Establish a connection to the Stelnet server 192.168.1.40:
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
   [SwitchA-Vlan-interface2] quit
   [SwitchA] quit

Before establishing a connection to the server, you can configure the server's host public key on the client to authenticate the server.

# To configure the server’s host public key on the client, perform the following tasks:
   # Use the display public-key local dsa public command on the server to display the server’s host public key. (Details not shown.)
   # Enter public key view of the client and copy the host public key of the server to the client.
   [SwitchA] public-key peer key1
   Enter public key view. Return to system view with "peer-public-key end" command.
   [SwitchA-pkey-public-key-key1]308201B73082012C06072A8648CE3804013082011F028181
   0D757262C4584C211F18BD96E5F0
   [SwitchA-pkey-public-key-key1]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CEC
   E65BE6C265854889DC1EDBD13EC8B274
# Establish an SSH connection to the server, and specify the host public key of the server.

```
<SwitchA> ssh2 192.168.1.40 publickey key1
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.
```

After you enter the correct password, you log in to Switch B successfully.

- If the client does not have the server's host public key, the system notifies you to confirm whether to continue with the access when you access the server. Select **Yes** to access the server and download the server's host public key.

```
<SwitchA> ssh2 192.168.1.40
```
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:y
client001@192.168.1.40's password:
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<SwitchB>
After you enter the correct password, you can log in to Switch B successfully. The server's
host public key is saved on the client. At the next connection attempt, the system will not
notify you to authenticate the server.

Publickey authentication enabled Stelnet client configuration example

Network requirements
As shown in Figure 105:
• You can log in to Switch B through the Stelnet client that runs on Switch A.
• After login, you are assigned the user role network-admin for configuration management.
• Switch B acts as the Stelnet server and uses publickey authentication and the DSA public key
algorithm.

Figure 105 Network diagram

Configuration procedure
In the server configuration, the client public key is required. Use the client software to generate a
DSA key pair on the client before configuring the Stelnet server.
1. Configure the Stelnet client:
   # Assign an IP address to VLAN-interface 2.
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
   [SwitchA-Vlan-interface2] quit
   # Generate a DSA key pair.
   [SwitchA] public-key local create dsa
   The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.................................................................
........+%..............................................+
................++.................................+
Create the key pair successfully.

# Export the DSA host public key to file key.pub.
[SwitchA] public-key local export dsa ssh2 key.pub
[SwitchA] quit

# Transmit the public key file key.pub to the server through FTP or TFTP. (Details not shown.)

2. Configure the Stelnet server:

# Generate RSA key pairs.
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key size is (512 ~ 2048)
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...

........................++++++
................++
.................++++++
............+++++
............++++
............++++
............++++
............++++
............++++
............++++
Create the key pair successfully.

# Generate a DSA key pair.
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...

........................++++++*
................++........+.................................+
................++........+.................................+
Create the key pair successfully.

# Generate an ECDSA key pair.
[SwitchB] public-key local create ecdsa secp256r1
Generating Keys...

Create the key pair successfully.

# Enable Stelnet server.
[SwitchB] ssh server enable

# Assign an IP address to VLAN-interface 2. The Stelnet client uses the address as the destination address of the SSH connection.
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
Stelnet configuration example based on 128-bit Suite B algorithms

Network requirements

As shown in Figure 106:

- Switch A acts as an Stelnet client (SSH2).
- Switch B acts as the Stelnet server (SSH2), and it uses publickey authentication.
- Switch B uses the following algorithms for the algorithm negotiation with the Stelnet client:
  - Key exchange algorithm **ecdh-sha2-nistp256**.
Encryption algorithm **aes128-gcm**.

Public key algorithms **x509v3-ecdsa-sha2-nistp256** and **x509v3-ecdsa-sha2-nistp384**.

Configure Switch A to establish a Stelnet connection to Switch B based on the 128-bit Suite B algorithms. After the connection is established, you can log in to Switch B from Switch A to configure and manage Switch B as an administrator.

**Figure 106 Network diagram**

**Configuration procedure**

1. Generate the client's certificate and the server's certificate. (Details not shown.)
   You must first configure the certificates of the server and the client because they are required for identity authentication between the two parties.
   In this example, the server's certificate file is `ssh-server-ecdsa256.p12` and the client's certificate file is `ssh-client-ecdsa256.p12`.

2. Configure the Stelnet client:

   **NOTE:**
   You can modify the pkix version of the client software OpenSSH to support Suite B. This example uses an HPE switch as an Stelnet client.

   ...
Subject: C=CN, ST=BJ, O-AA, OU=Software, CN=SSH Server secp256

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

3c:9e:a2:b7:83:87:b9:ad:28:c8:2a:5e:58:11:8e:
c7:61:4a:52:51

ASN1 OID: prime256v1

NIST CURVE: P-256

X509v3 extensions:

X509v3 Basic Constraints:
CA:FALSE

Netscape Comment:
OpenSSL Generated Certificate

X509v3 Subject Key Identifier:


X509v3 Authority Key Identifier:


Signature Algorithm: ecdsa-with-SHA256


# Create a PKI domain named client256 for the client's certificate and enter its view.

[SwitchA] pki domain client256

# Disable CRL checking.

[SwitchA-pki-domain-client256] undo crl check enable

[SwitchA-pki-domain-client256] quit

# Import the local certificate file ssh-client-ecdsa256.p12 to PKI domain client256.

[SwitchA] pki import domain client256 p12 local filename ssh-client-ecdsa256.p12

The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).

Please enter the key pair name[default name: client256]:

# Display information about local certificates in PKI domain client256.

[SwitchA] display pki certificate domain client256 local

Certificate:

Data:

Version: 3 (0x2)
Serial Number: 4 (0x4)
Signature Algorithm: ecdsa-with-SHA256
Issuer: C=CN, ST=BJ, L=BJ, O-AA, OU=Software, CN=SuiteB CA
Validity
Not Before: Aug 21 08:41:09 2015 GMT
Not After : Aug 20 08:41:09 2016 GMT
Subject: C=CN, ST=BJ, O=AA, OU=Software, CN=SSH Client secp256
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (256 bit)
pub:
12:d0:b4:8a:92
ASN1 OID: prime256v1
NIST CURVE: P-256
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
X509v3 Authority Key Identifier:
Signature Algorithm: ecdsa-with-SHA256
31:00:3a:af:2a:8f:d6:8d:1f:3a:2b:ae:2f:97:b3:52:63:b6:

# Assign an IP address to VLAN-interface 2.
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[SwitchA-Vlan-interface2] quit

3. Configure the Stelnet server:

   # Upload the server's certificate file ssh-server-ecdsa256.p12 and the client's certificate file ssh-client-ecdsa256.p12 to the Stelnet server through FTP or TFTP. (Details not shown.)
   # Create a PKI domain named client256 for verifying the client's certificate and import the file of the client's certificate to this domain. (Details not shown.)
   # Create a PKI domain named server256 for the server's certificate and import the file of the server's certificate to this domain. (Details not shown.)
   # Specify Suite B algorithms for algorithm negotiation.

<SwitchB> system-view
[SwitchB] ssh2 algorithm key-exchange ecdh-sha2-nistp256
[SwitchB] ssh2 algorithm cipher aes128-gcm
[SwitchB] ssh2 algorithm public-key x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384

# Specify server256 as the PKI domain of the server's certificate.
[SwitchB] ssh server pki-domain server256

# Enable the Stelnet server.
[SwitchB] ssh server enable

# Assign an IP address to VLAN-interface 2.
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[SwitchB-Vlan-interface2] quit

# Set the authentication mode to AAA for user lines.
[SwitchB] line vty 0 63
[SwitchB-line-vty0-63] authentication-mode scheme
[SwitchB-line-vty0-63] quit

# Create a local device management user named client001. Authorize the user to use the SSH service and assign the network-admin user role to the user.
[SwitchB] local-user client001 class manage
[SwitchB-luser-manage-client001] service-type ssh
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit

# Create an SSH user named client001. Specify the authentication method publickey for the user and specify client256 as the PKI domain for verifying the client's certificate.
[Switch] ssh user client001 service-type stelnet authentication-type publickey assign pki-domain client256


<SwitchA>  ssh2 192.168.1.40 suite-b 128-bit pki-domain client256 server-pki-domain server256

Username: client001
Press CTRL+C to abort.

Connecting to 192.168.1.40 port 22.
Enter a character ~ and a dot to abort.

******************************************************************************
* Copyright (c) 2010-2016 Hewlett Packard Enterprise Development LP          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<SwitchB>

SFTP configuration examples

Devices in the configuration examples are in non-FIPS mode.

When you configure SFTP on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of RSA key pairs must be 2048 bits.
When the device acts as the SFTP server, it supports only ECDSA and RSA key pairs. If both ECDSA and RSA key pairs exist on the server, the server uses the ECDSA key pair.

Password authentication enabled SFTP server configuration example

Network requirements

As shown in Figure 107:

- You can log in to the switch through the SFTP client that runs on the host.
- After login, you are assigned the user role network-admin to execute file management and transfer operations.
- The switch acts as the SFTP server and uses password authentication.
- The username and password of the client are saved on the switch.

![Figure 107 Network diagram](image)

Configuration procedure

1. Configure the SFTP server:

   # Generate RSA key pairs.
   <Switch> system-view
   [Switch] public-key local create rsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   .........+++++++      
   .........+++++++     
   .........+++++++    
   .........+++++++   
   Create the key pair successfully.

   # Generate a DSA key pair.
   [Switch] public-key local create dsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   +++++++++++++++++++*
   +...............+.....+...........................+
   +...............+.........+................++
   Create the key pair successfully.

   # Generate an ECDSA key pair.
Switch public-key local create ecdsa secp256r1
Generating Keys...

Create the key pair successfully.

# Enable the SFTP server.
[Switch] sftp server enable

# Assign an IP address to VLAN-interface 2. The SFTP client uses the address as the destination for SSH connection.
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface2] quit

# Create a local device management user client002. Specify the plaintext password as aabbcc and the service type as ssh for the user. Assign the user role network-admin and the working directory flash:/ to the user.
[Switch] local-user client002 class manage
[Switch-luser-manage-client002] password simple aabbcc
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
work-directory flash:/
[Switch-luser-manage-client002] quit

# Create an SSH user client002. Specify the authentication method as password and the service type as sftp for the user.
[Switch] ssh user client002 service-type sftp authentication-type password

2. Establish a connection between the SFTP client and the SFTP server:
The device supports different types of SFTP client software. This example uses an SFTP client that runs PSFTP of PuTTY version 0.58.

**NOTE:**
PSFTP supports only password authentication.

To establish a connection to the SFTP server:

a. Run the psftp.exe to launch the client interface shown in Figure 108, and enter the following command:
   open 192.168.1.45

b. Enter username client002 and password aabbcc as prompted to log in to the SFTP server.
Publickey authentication enabled SFTP client configuration example

Network requirements

As shown in Figure 109:

- You can log in to Switch B through the SFTP client that runs on Switch A.
- After login, you are assigned the user role network-admin to execute file management and transfer operations.
- Switch B acts as the SFTP server and uses publickey authentication and the RSA public key algorithm.

Configuration procedure

In the server configuration, the client's host public key is required. Generate RSA key pairs on the client before configuring the SFTP server.

1. Configure the SFTP client:

   # Assign an IP address to VLAN-interface 2.
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
   [SwitchA-Vlan-interface2] quit

   # Generate RSA key pairs.
[SwitchA] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...

.........................+++++
.........................+++++
........+................++++
Create the key pair successfully.

# Export the host public key to the file pubkey.
[SwitchA] public-key local export rsa ssh2 pubkey
[SwitchA] quit

# Transmit the public key file pubkey to the server through FTP or TFTP. (Details not shown.)

2. Configure the SFTP server:
   # Generate RSA key pairs.
   <SwitchB> system-view
   [SwitchB] public-key local create rsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...

.................................+++++
.................................+++++
................+................++++
Create the key pair successfully.

# Generate a DSA key pair.
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...

.................................+++++
.................................+++++
........+................+...........
Create the key pair successfully.

# Generate an ECDSA key pair.
[SwitchB] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.

# Enable the SFTP server.
[SwitchB] sftp server enable
# Assign an IP address to VLAN-interface 2. The SFTP client uses the address as the destination for SSH connection.

```bash
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

# Import the peer public key from the file `pubkey`, and name it `switchkey`.

```bash
[SwitchB] public-key peer switchkey import sshkey pubkey
```

# Create an SSH user `client001`. Specify the service type as `sftp` and the authentication method as `publickey` for the user. Assign the public key `switchkey` to the user.

```bash
[SwitchB] ssh user client001 service-type sftp authentication-type publickey assign publickey switchkey
```

# Create a local device management user `client001`.

```bash
[SwitchB] local-user client001 class manage
```

# Specify the service type as `ssh` for the user.

```bash
[SwitchB-luser-manage-client001] service-type ssh
```

# Assign the user role `network-admin` and the working directory `flash:` to the user.

```bash
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin work-directory flash:
```

```bash
[SwitchB-luser-manage-client001] quit
```

3. Establish a connection to the SFTP server:

# Establish a connection to the SFTP server and enter SFTP client view.

```bash
<SwitchA> sftp 192.168.0.1 identity-key rsa
```

Username: client001

Press CTRL+C to abort.

Connecting to 192.168.0.1 port 22.

The server is not authenticated. Continue? [Y/N]: y

Do you want to save the server public key? [Y/N]: n

sftp>

# Display files under the current directory of the server, delete the file `z`, and verify the result.

```bash
sftp> dir -l
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub
-rwxrwxrwx 1 noone nogroup 0 Sep 01 08:00 z
```

sftp> delete z

Removing /z

```bash
sftp> dir -l
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub
```

# Add a directory `new1` and verify the result.

```bash
sftp> mkdir new1
```

```bash
sftp> dir -l
-rwxrwxrwx 1 noone nogroup 1759 Aug 23 06:52 config.cfg
-rwxrwxrwx 1 noone nogroup 225 Aug 24 08:01 pubkey2
-rwxrwxrwx 1 noone nogroup 283 Aug 24 07:39 pubkey
drwxrwxrwx 1 noone nogroup 0 Sep 01 06:22 new
-rwxrwxrwx 1 noone nogroup 225 Sep 01 06:55 pub
```
SFTP configuration example based on 192-bit Suite B algorithms

Network requirements

As shown in Figure 110:

- Switch A acts as an SFTP client (SSH2).
- Switch B acts as the SFTP server (SSH2), and it uses publickey authentication.
- Switch B uses the following algorithms for the algorithm negotiation with the SFTP client:
  - Key exchange algorithm `ecdh-sha2-nistp384`.
  - Encryption algorithm `aes256-gcm`.
  - Public key algorithm `x509v3-ecdsa-sha2-nistp384`. 
Configure Switch A to establish an SFTP connection to Switch B based on the 192-bit Suite B algorithms. After the connection is established, you can log in to Switch B from Switch A to manage and transfer files as an administrator.

Figure 110 Network diagram

**Configuration procedure**

1. Generate the client's certificate and the server's certificate. (Details not shown.)
   
   You must first configure the certificates of the server and the client because they are required for identity authentication between the two parties.

   In this example, the server's certificate file is `ssh-server-ecdsa384.p12` and the client's certificate file is `ssh-client-ecdsa384.p12`.

2. Configure the SFTP client:

   **NOTE:**

   You can modify the pkix version of the client software OpenSSH to support Suite B. This example uses an HPE switch as an SFTP client.

   ```
   # Upload the server's certificate file `ssh-server-ecdsa384.p12` and the client's certificate file `ssh-client-ecdsa384.p12` to the SFTP client through FTP or TFTP. (Details not shown.)
   # Create a PKI domain named `server384` for verifying the server's certificate and enter its view.
   <SwitchA> system-view
   [SwitchA] pki domain server384
   # Disable CRL checking.
   [SwitchA-pki-domain-server384] undo crl check enable
   [SwitchA-pki-domain-server384] quit
   # Import the local certificate file `ssh-server-ecdsa384.p12` to PKI domain `server384`.
   [SwitchA] pki import domain server384 p12 local filename ssh-server-ecdsa384.p12
   The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).
   Please enter the key pair name [default name: server384]:
   # Display information about local certificates in PKI domain `server384`.
   [SwitchA] display pki certificate domain server384 local
   Certificate:
   Data:
   Version: 3 (0x2)
   Serial Number: 1 (0x1)
   Signature Algorithm: ecdsa-with-SHA384
   Issuer: C=CN, ST=BJ, L=BJ, O=AA, OU=Software, CN=SuiteB CA
   Validity
   Not Before: Aug 20 10:08:41 2015 GMT
   Not After : Aug 19 10:08:41 2016 GMT
   Subject: C=CN, ST=BJ, O=AA, OU=Software, CN=ssh server
   Subject Public Key Info:
   Public Key Algorithm: id-ecPublicKey
   ```
Public-Key: (384 bit)

pub:

b6:36:el:4d:cc:8c:05:22:ff:3a:7c:5d:b7:be:d1:
07:01:f9:fc:a5:6f:81

ASN1 OID: secp384r1
NIST CURVE: P-384
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
X509v3 Authority Key Identifier:

Signature Algorithm: ecdsa-with-SHA384

# Create a PKI domain named client384 for the client's certificate and enter its view.
[SwitchA] pki domain client384

# Disable CRL checking.
[SwitchA-pki-domain-client384] undo crl check enable
[SwitchA-pki-domain-client384] quit

# Import the local certificate file ssh-client-ecdsa384.p12 to PKI domain client384.
[SwitchA] pki import domain client384 p12 local filename ssh-client-ecdsa384.p12
The system is going to save the key pair. You must specify a key pair name, which is
a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A
to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: client384]:

# Display information about local certificates in PKI domain client384.
[SwitchA] display pki certificate domain client384 local
Not Before: Aug 20 10:10:59 2015 GMT  
Not After : Aug 19 10:10:59 2016 GMT  
Subject: C=CN, ST=BJ, O=AA, OU=Software, CN=ssh client  
Subject Public Key Info:  
Public Key Algorithm: id-ecPublicKey  
Public-Key: (384 bit)  
pub:  
91:70:31:2a:92:00:76  
ASN1 OID: secp384r1  
NIST CURVE: P-384  
X509v3 extensions:  
X509v3 Basic Constraints:  
CA:FALSE  
Netscape Comment:  
OpenSSL Generated Certificate  
X509v3 Subject Key Identifier:  
X509v3 Authority Key Identifier:  
Signature Algorithm: ecdsa-with-SHA384  
30:66:02:31:00:6d:0a:27:80:19:0f:22:db:5b:40:00:fa:02: 
31:00:ee:00:e1:07:0c:2f:12:3f:88:ea:fe:19:05:ef:56:ca: 

# Assign an IP address to VLAN-interface 2.  
[SwitchA] interface vlan-interface 2  
[SwitchA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0  
[SwitchA-Vlan-interface2] quit  
[SwitchA] quit  

3. Configure the SFTP server:  
# Upload the server's certificate file ssh-server-ecdsa384.p12 and the client's certificate file ssh-client-ecdsa384.p12 to the SFTP server through FTP or TFTP. (Details not shown.)  
# Create a PKI domain named client384 for verifying the client's certificate and import the file of the client's certificate to this domain. (Details not shown.)  
# Create a PKI domain named server384 for the server's certificate and import the file of the server's certificate to this domain. (Details not shown.)  
# Specify Suite B algorithms for algorithm negotiation.  
[SwitchB] ssh2 algorithm key-exchange ecdh-sha2-nistp384  
[SwitchB] ssh2 algorithm cipher aes256-gcm
[SwitchB] ssh2 algorithm public-key x509v3-ecdsa-sha2-nistp384
# Specify server384 as the PKI domain of the server's certificate.
[SwitchB] ssh server pki-domain server384
# Enable the SFTP server.
[SwitchB] sftp server enable
# Assign an IP address to VLAN-interface 2.
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
# Set the authentication mode to AAA for user lines.
[SwitchB] line vty 0 63
[SwitchB-line-vty0-63] authentication-mode scheme
[SwitchB-line-vty0-63] quit
# Create a local device management user named client001. Authorize the user to use the SSH service and assign the network-admin user role to the user.
[SwitchB] local-user client001 class manage
[SwitchB-luser-manage-client001] service-type ssh
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit
# Create an SSH user named client001. Specify the authentication method publickey for the user and specify client384 as the PKI domain for verifying the client's certificate.
[Switch] ssh user client001 service-type sftp authentication-type publickey assign pki-domain client384

4. Establish an SFTP connection to SFTP server 192.168.0.1 based on the 192-bit Suite B algorithms.

   <SwitchA> sftp 192.168.0.1 suite-b 192-bit pki-domain client384 server-pki-domain server384
   Username: client001
   Press CTRL+C to abort.
   Connecting to 192.168.0.1 port 22.
   sftp>

SCP configuration examples

Devices in the configuration examples are in non-FIPS mode.

When you configure SCP on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of RSA key pairs must be 2048 bits.
- When the device acts as an SCP server, only ECDSA and RSA key pairs are supported. If both ECDSA and RSA key pairs exist on the server, the server uses the ECDSA key pair.

SCP file transfer with password authentication

Network requirements

As shown in Figure 111:

- You can log in to Switch B through the SCP client that runs on Switch A.
• After login, you are assigned the user role **network-admin** and can securely transfer files with Switch B.
• Switch B uses the password authentication method.
• The client's username and password are saved on Switch B.

**Figure 111 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. Configure the SCP server:
   
   # Generate RSA key pairs.
   ```
   <SwitchB> system-view
   [SwitchB] public-key local create rsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   .........................++++++
   .........................++++++
   .................++++++
   Create the key pair successfully.
   # Generate a DSA key pair.
   [SwitchB] public-key local create dsa
   The range of public key size is (512 ~ 2048).
   If the key modulus is greater than 512, it will take a few minutes.
   Press CTRL+C to abort.
   Input the modulus length [default = 1024]:
   Generating Keys...
   +.................................................................+
   +............................+++++
   +............................+++++
   Create the key pair successfully.
   # Generate an ECDSA key pair.
   [SwitchB] public-key local create ecdsa secp256r1
   Generating Keys...
   Create the key pair successfully.
   # Enable the SCP server.
   [SwitchB] scp server enable
   # Configure an IP address for VLAN-interface 2. The SCP client uses this address as the destination for SCP connection.
   [SwitchB] interface vlan-interface 2
   [SwitchB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface2] quit

# Create a local device management user client001.
[SwitchB] local-user client001 class manage

# Specify the plaintext password as aabbcc and the service type as ssh for the user.
[SwitchB-luser-manage-client001] password simple aabbcc
[SwitchB-luser-manage-client001] service-type ssh

# Assign the user role network-admin to the user.
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit

# Configure an SSH user client001. Specify the service type as scp and the authentication method as password for the user.
[SwitchB] ssh user client001 service-type scp authentication-type password

2. Configure an IP address for VLAN-interface 2 on the SCP client.
   <SwitchA> system-view
   [SwitchA] interface vlan-interface 2
   [SwitchA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
   [SwitchA-Vlan-interface2] quit
   [SwitchA] quit

3. Connect to the SCP server, download the file remote.bin from the server, and save it locally with the name local.bin.
   <SwitchA> scp 192.168.0.1 get remote.bin local.bin
   Username: client001
   Press CTRL+C to abort.
   Connecting to 192.168.0.1 port 22.
   The server is not authenticated. Continue? [Y/N]:y
   Do you want to save the server public key? [Y/N]:n
   client001@192.168.0.1’s password:
   remote.bin 100% 2875 2.8KB/s 00:00

SCP configuration example based on Suite B algorithms

Network requirements

As shown in Figure 112:

- Switch A acts as an SCP client (SSH2).
- Switch B acts as the SCP server (SSH2), and it uses publickey authentication.
- Switch B uses the following algorithms for the algorithm negotiation with the SCP client:
  - Key exchange algorithms ecdh-sha2-nistp256 and ecdh-sha2-nistp384.
  - Encryption algorithms aes128-gcm and aes256-gcm.
  - Public key algorithms x509v3-ecdsa-sha2-nistp256 and x509v3-ecdsa-sha2-nistp384.

Configure Switch A to establish an SCP connection to Switch B based on the Suite B algorithms. After the connection is established, you can log in to Switch B from Switch A to transfer files between switches as an administrator.
**Configuration procedure**

1. Generate the client's certificates and the server's certificates. (Details not shown.)
   - You must first configure the certificates of the server and the client because they are required for identity authentication between the two parties.
   - In this example, the server's certificate files are `ssh-server-ecdsa256.p12` and `ssh-server-ecdsa384.p12`. The client's certificate files are `ssh-client-ecdsa256.p12` and `ssh-client-ecdsa384.p12`.

2. Configure the SCP client:

   **NOTE:**
   - You can modify the pkix version of the client software OpenSSH to support Suite B. This example uses an HPE switch as an SCP client.

   ```
   # Upload the server's certificate files (ssh-server-ecdsa256.p12 and ssh-server-ecdsa384.p12) and the client's certificate files (ssh-client-ecdsa256.p12 and ssh-client-ecdsa384.p12) to the SCP client through FTP or TFTP. (Details not shown.)
   # Create a PKI domain named server256 for verifying the server's certificate ecdsa256 and enter its view.
   <SwitchA> system-view
   [SwitchA] pki domain server256
   # Disable CRL checking.
   [SwitchA-pki-domain-server256] undo crl check enable
   [SwitchA-pki-domain-server256] quit
   # Import the local certificate file ssh-server-ecdsa256.p12 to PKI domain server256.
   [SwitchA] pki import domain server256 p12 local filename ssh-server-ecdsa256.p12
   # Display information about local certificates in PKI domain server256.
   [SwitchA] display pki certificate domain server256 local
   Certificate:
   Data:
   Version: 3 (0x2)
   Serial Number: 3 (0x3)
   Signature Algorithm: ecdsa-with-SHA256
   Issuer: C=CN, ST=BJ, L=BJ, O=AA, OU=Software, CN=SuiteB CA
   Validity
   Not Before: Aug 21 08:39:51 2015 GMT
   Not After : Aug 20 08:39:51 2016 GMT
   Subject: C=CN, ST=BJ, O=AA, OU=Software, CN=SSH Server secp256
   Subject Public Key Info:
   Public Key Algorithm: id-ecPublicKey
   ```
Public-Key: (256 bit)

pub:
3c:9e:a2:b7:83:87:b9:ad:28:c8:2a:5e:58:11:8e:
c7:61:4a:52:51
ASN1 OID: prime256v1
NIST CURVE: P-256
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
Netscape Comment:
  OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
X509v3 Authority Key Identifier:

Signature Algorithm: ecdsa-with-SHA256

# Create a PKI domain named client256 for the client's certificate ecdsa256 and enter its view.

[SwitchA] pki domain client256

# Disable CRL checking.

[SwitchA-pki-domain-client256] undo crl check enable
[SwitchA-pki-domain-client256] quit

# Import the local certificate file ssh-client-ecdsa256.p12 to PKI domain client256.

[SwitchA] pki import domain client256 p12 local filename ssh-client-ecdsa256.p12

The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).

Please enter the key pair name[default name: client256]:

# Display information about local certificates in PKI domain client256.

[SwitchA] display pki certificate domain client256 local

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 4 (0x4)
Signature Algorithm: ecdsa-with-SHA256
  Issuer: C=CN, ST=BJ, L=BJ, O=AA, OU=Software, CN=SuiteB CA
  Validity
    Not Before: Aug 21 08:41:09 2015 GMT
    Not After : Aug 20 08:41:09 2016 GMT
Subject: C=CN, ST=BJ, O=AA, OU=Software, CN=SSH Client secp256
Subject Public Key Info:
  Public Key Algorithm: id-ecPublicKey
  Public-Key: (256 bit)
  pub:
    12:d0:b4:8a:92
  ASN1 OID: prime256v1
  NIST CURVE: P-256

X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
  X509v3 Subject Key Identifier:
  X509v3 Authority Key Identifier:

Signature Algorithm: ecdsa-with-SHA256

# Create a PKI domain named server384 for verifying the server's certificate ecdsa384 and enter its view.
[SwitchA] pki domain server384

# Disable CRL checking.
[SwitchA-pki-domain-server384] undo crl check enable
[SwitchA-pki-domain-server384] quit

# Import the local certificate file ssh-server-ecdsa384.p12 to PKI domain server384.
[SwitchA] pki import domain server384 p12 local filename ssh-server-ecdsa384.p12
The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: server384]:

# Display information about local certificates in PKI domain server384.
[SwitchA] display pki certificate domain server384 local
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: ecdsa-with-SHA384
Issuer: C=CN, ST=BJ, L=BJ, O=AA, OU=Software, CN=SuiteB CA
Validity
Not Before: Aug 20 10:08:41 2015 GMT
Not After : Aug 19 10:08:41 2016 GMT
Subject: C=CN, ST=BJ, O=AA, OU=Software, CN=ssh server
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (384 bit)
  pub:
  07:01:f9:dc:a5:6f:81
ASN1 OID: secp384r1
NIST CURVE: P-384
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
X509v3 Authority Key Identifier:
Signature Algorithm: ecdsa-with-SHA384

# Create a PKI domain named client384 for the client's certificate ecdsa384 and enter its view.
[SwitchA] pki domain client384

# Disable CRL checking.
[SwitchA-pki-domain-client384] undo crl check enable
[SwitchA-pki-domain-client384] quit

# Import the local certificate file ssh-client-ecdsa384.p12 to PKI domain client384.
[SwitchA] pki import domain client384 p12 local filename ssh-client-ecdsa384.p12
The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: client384]:

# Display information about local certificates in PKI domain client384.
[SwitchA] display pki certificate domain client384 local
Certificate:

Data:

Version: 3 (0x2)
Serial Number: 2 (0x2)
Signature Algorithm: ecdsa-with-SHA384
Issuer: C=CN, ST=BJ, L=BJ, O=AA, OU=Software, CN=SuiteB CA

Validity

Not Before: Aug 20 10:10:59 2015 GMT
Not After : Aug 19 10:10:59 2016 GMT
Subject: C=CN, ST=BJ, O=AA, OU=Software, CN=ssh client
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (384 bit)
pub:
91:70:31:2a:92:00:76
ASN1 OID: secp384r1
NIST CURVE: P-384
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
X509v3 Authority Key Identifier:

Signature Algorithm: ecdsa-with-SHA384
30:66:02:31:00:12:06:fa:2c:0b:0d:ff:81:90:01:0c:3:3:db:
31:00:ee:00:e1:07:c0:2f:12:3f:88:ea:fe:19:05:ef:56:ca:

# Assign an IP address to VLAN-interface 2.
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface2] quit

3. Configure the SCP server:

# Upload the server's certificate files (ssh-server-ecdsa256.p12 and ssh-server-ecdsa384.p12) and the client's certificate files (ssh-client-ecdsa256.p12 and ssh-client-ecdsa384.p12) to the SCP server through FTP or TFTP. (Details not shown.)
# Create a PKI domain named \texttt{client256} for verifying the client's certificate \texttt{ecdsa256} and import the file of this certificate to this domain. Create a PKI domain named \texttt{server256} for the server's certificate \texttt{ecdsa256} and import the file of this certificate to this domain. (Details not shown.)

# Create a PKI domain named \texttt{client384} for verifying the client's certificate \texttt{ecdsa384} and import the file of this certificate to this domain. Create a PKI domain named \texttt{server384} for the server's certificate \texttt{ecdsa384} and import the file of this certificate to this domain. (Details not shown.)

# Specify Suite B algorithms for algorithm negotiation.

```plaintext
<SwitchB> system-view
[SwitchB] ssh2 algorithm key-exchange ecdh-sha2-nistp256 ecdh-sha2-nistp384
[SwitchB] ssh2 algorithm cipher aes128-gcm aes256-gcm
[SwitchB] ssh2 algorithm public-key x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
```

# Enable the SCP server.

```plaintext
[SwitchB] scp server enable
```

# Assign an IP address to VLAN-interface 2.

```plaintext
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
```

# Set the authentication mode to AAA for user lines.

```plaintext
[SwitchB] line vty 0 63
[SwitchB-line-vty0-63] authentication-mode scheme
[SwitchB-line-vty0-63] quit
```

# Create a local device management user named \texttt{client001}. Authorize the user to use the SSH service and assign the \texttt{network-admin} user role to the user.

```plaintext
[SwitchB] local-user client001 class manage
[SwitchB-luser-manage-client001] service-type ssh
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit
```

# Create a local device management user named \texttt{client002}. Authorize the user to use the SSH service and assign the \texttt{network-admin} user role to the user.

```plaintext
[SwitchB] local-user client002 class manage
[SwitchB-luser-manage-client002] service-type ssh
[SwitchB-luser-manage-client002] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client002] quit
```

4. Establish an SCP connection to SCP server \texttt{192.168.0.1}:

   - Based on the 128-bit Suite B algorithms:
     ```plaintext
     # Specify \texttt{server256} as the PKI domain of the server's certificate.
     [SwitchB] ssh server pki-domain server256
     # Create an SSH user named \texttt{client001}. Specify the authentication method \texttt{publickey} for the user and specify \texttt{client256} as the PKI domain for verifying the client's certificate.
     [Switch] ssh user client001 service-type scp authentication-type publickey assign pki-domain client256
     # Establish an SCP connection to SCP server \texttt{192.168.0.1} based on the 128-bit Suite B algorithms.
     <SwitchA> scp 192.168.0.1 get src.cfg suite-b 128-bit pki-domain client256 server-pki
     -domain server256
     ```
Based on the 192-bit Suite B algorithms:

# Specify server384 as the PKI domain of the server's certificate.

[SwitchB] ssh server pki-domain server384

# Create an SSH user named client002. Specify the authentication method publickey for the user and specify client384 as the PKI domain for verifying the client's certificate.

[Switch] ssh user client002 service-type scp authentication-type publickey assign pki-domain client384

# Establish an SCP connection to SCP server 192.168.0.1 based on the 192-bit Suite B algorithms.

<SwitchA> scp 192.168.0.1 get src.cfg suite-b 192-bit pki-domain client384 server-pki
                   -domain server384
Username: client002
Press CTRL+C to abort.
Connecting to 192.168.0.1 port 22.
src.cfg                                       100% 4814     4.7KB/s   00:00
<SwitchA>

NETCONF over SSH configuration example with password authentication

The switch in the configuration example is in non-FIPS mode.

When you configure NETCONF-over-SSH on a device that operates in FIPS mode, follow these restrictions and guidelines:

- The modulus length of RSA key pairs must be 2048 bits.
- When the device acts as the NETCONF-over-SSH server, it supports only ECDSA and RSA key pairs. If both ECDSA and RSA key pairs exist on the server, the server uses the ECDSA key pair.

Network requirements

As shown in Figure 113:

- The switch uses local password authentication.
- The client's username and password are saved on the switch.

Establish a NETCONF-over-SSH connection between the host and the switch, so that you can log in to the switch from the host to perform NETCONF operations.
Figure 113 Network diagram

```
# Generate RSA key pairs.
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
........................++++++
...................++++++
..++++++++
............++++++++
.........+++++++
Create the key pair successfully.

# Generate a DSA key pair.
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
........................++++++*
...................++++++
...+.................+..........+...+
Create the key pair successfully.

# Generate an ECDSA key pair.
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.

# Enable NETCONF over SSH.
[Switch] netconf ssh server enable

# Configure an IP address for VLAN-interface 2. The client uses this address as the destination for NETCONF-over-SSH connection.
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit

# Set the authentication mode to AAA for the user lines.
[Switch] line vty 0 63
```


```bash
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit

# Create a local device management user client001.
[Switch] local-user client001 class manage

# Specify the plaintext password as aabbcc and the service type as ssh for the user.
[Switch-luser-manage-client001] password simple aabbcc
[Switch-luser-manage-client001] service-type ssh

# Assign the user role network-admin to the user.
[Switch-luser-manage-client001] authorization-attribute user-role network-admin

# Configure an SSH user client001. Specify the service type as NETCONF and the authentication method as password for the user.
[Switch] ssh user client001 service-type netconf authentication-type password
```

Verifying the configuration

# Verify that you can perform NETCONF operations after logging in to the switch. (Details not shown.)
Configuring SSL

Overview

Secure Sockets Layer (SSL) is a cryptographic protocol that provides communication security for TCP-based application layer protocols such as HTTP. SSL has been widely used in applications such as e-business and online banking to provide secure data transmission over the Internet.

SSL security services

SSL provides the following security services:

- **Privacy**—SSL uses a symmetric encryption algorithm to encrypt data and uses an asymmetric key algorithm such as RSA to encrypt the key used by the symmetric encryption algorithm. For more information about RSA, see "Managing public keys."

- **Authentication**—SSL uses certificate-based digital signatures to authenticate the SSL server and client. The SSL server and client obtain digital certificates through PKI. For more information about PKI and digital certificates, see "Configuring PKI."

- **Integrity**—SSL uses the message authentication code (MAC) to verify message integrity. It uses a MAC algorithm and a key to transform a message of any length to a fixed-length message. Any change to the original message will result in a change to the calculated fixed-length message. As shown in Figure 114, the message integrity verification process is as follows:
  
a. The sender uses a MAC algorithm and a key to calculate a MAC value for a message. Then, it appends the MAC value to the message, and sends the message to the receiver.

b. The receiver uses the same key and MAC algorithm to calculate a MAC value for the received message, and compares it with the MAC value appended to the message.

c. If the two MAC values match, the receiver considers the message intact. Otherwise, the receiver considers that the message was tampered with and it discards the message.

Figure 114 MAC algorithm diagram

SSL protocol stack

The SSL protocol stack includes the following protocols:

- SSL record protocol at the lower layer.
- SSL handshake protocol, SSL change cipher spec protocol, and SSL alert protocol at the upper layer.
The following describes the major functions of SSL protocols:

- **SSL record protocol**—Fragments data received from the upper layer, computes and adds MAC to the data, and encrypts the data.

- **SSL handshake protocol**—Negotiates the cipher suite used for secure communication, authenticates the server and client, and securely exchanges the keys between the server and client. The cipher suite that needs to be negotiated includes the symmetric encryption algorithm, key exchange algorithm, and MAC algorithm.

- **SSL change cipher spec protocol**—Notifies the receiver that subsequent packets are to be protected based on the negotiated cipher suite and key.

- **SSL alert protocol**—Sends alert messages to the receiving party. An alert message contains the alert severity level and a description.

### FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode (see "Configuring FIPS") and non-FIPS mode.

### SSL configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring an SSL server policy</td>
<td>Perform this configuration task on the SSL server.</td>
</tr>
<tr>
<td>Configuring an SSL client policy</td>
<td>Perform this configuration task on the SSL client.</td>
</tr>
</tbody>
</table>

### Configuring an SSL server policy

An SSL server policy is a set of SSL parameters used by the SSL server. An SSL server policy takes effect only after it is associated with an application such as HTTPS.

SSL protocol versions include SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. By default:

- In Release 1111, the SSL server can communicate with clients running SSL 3.0 and TLS 1.0. When the server receives an SSL 2.0 Client Hello message from a client, it notifies the client to use SSL 3.0 or TLS 1.0 for communication.

- In Release 1121 and later, the SSL server can communicate with clients running all SSL protocol versions. When the server receives an SSL 2.0 Client Hello message from a client, it notifies the client to use a later version for communication.

You can disable specific SSL protocol versions on the device to enhance system security.

To configure an SSL server policy:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Disable specific SSL protocol versions on the device.</td>
<td>If Release 1111, SSL 3.0 is enabled on the device by default. In Release 1121 and later, the default setting is as follows: • In non-FIPS mode, the device supports SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. • In FIPS mode, the device supports TLS 1.0, TLS 1.1, and TLS 1.2.</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Disable SSL session renegotiation.</td>
<td>By default, SSL session renegotiation is enabled. This command is available in Release 1121 and later.</td>
</tr>
<tr>
<td>4.</td>
<td>Create an SSL server policy and enter its view.</td>
<td>By default, no SSL server policies exist on the device.</td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Specify a PKI domain for the SSL server policy.</td>
<td>By default, no PKI domain is specified for an SSL server policy. If SSL server authentication is required, you must specify a PKI domain and request a local certificate for the SSL server in the domain. For information about how to create and configure a PKI domain, see &quot;Configuring PKI.&quot;</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the cipher suites that the SSL server policy supports.</td>
<td>By default, an SSL server policy supports all cipher suites.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>7.</td>
<td><strong>session cachesize</strong> <em>size</em></td>
<td>By default, an SSL server can cache a maximum of 500 sessions.</td>
</tr>
<tr>
<td>8.</td>
<td><strong>client-verify enable</strong></td>
<td>By default, SSL client authentication is disabled.</td>
</tr>
</tbody>
</table>
**Configuring an SSL client policy**

An SSL client policy is a set of SSL parameters that the client uses to establish a connection to the server. An SSL client policy takes effect only after it is associated with an application such as DDNS.

In Release 1111, you can specify the SSL 3.0 or TLS 1.0 for an SSL client policy:

- If TLS 1.0 is specified and SSL 3.0 is not disabled, the client first uses TLS 1.0 to connect to the SSL server. If the connection attempt fails, the client uses SSL 3.0.
- If TLS 1.0 is specified and SSL 3.0 is disabled, the client only uses TLS 1.0 to connect to the SSL server.
- If SSL 3.0 is specified, the client uses SSL 3.0 to connect to the SSL server, whether you disable SSL 3.0 or not.

As a best practice to enhance system security, disable SSL 3.0 on the device and specify TLS 1.0 for an SSL client policy.

In Release 1121 and later, the SSL client always uses the SSL protocol version specified for it, whether you disable the SSL protocol version or not.

To configure an SSL client policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Disable SSL session renegotiation.</td>
<td>ssl renegotiation disable</td>
</tr>
<tr>
<td>3.</td>
<td>Create an SSL client policy and enter its view.</td>
<td>ssl client-policy policy-name</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Specify a PKI domain for the SSL client policy.</td>
<td>pki-domain domain-name</td>
</tr>
</tbody>
</table>

5. Specify the preferred cipher suite for the SSL client policy.

In Release 1111:
- In non-FIPS mode: prefer-cipher { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 | rsa_3des_ebe_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha }
- In FIPS mode:

In non-FIPS mode: The default preferred cipher suite is **rsa_rc4_128_md5**.
- In FIPS mode: The default preferred cipher suite is **rsa_aes_128_cbc_sha**.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>prefer-cipher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>{ dhe_rsa_aes_128_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dhe_rsa_aes_256_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_aes_128_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_aes_256_cbc_sha }</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Release 1121 and later:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• In non-FIPS mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefer-cipher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>{ dhe_rsa_aes_128_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dhe_rsa_aes_128_cbc_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dhe_rsa_aes_256_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dhe_rsa_aes_256_cbc_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_ecdsa_aes_128_cbc_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_ecdsa_aes_128_gcm_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_ecdsa_aes_128_cbc_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_ecdsa_aes_256_cbc_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_rsa_aes_128_cbc_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_rsa_aes_128_gcm_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_rsa_aes_256_cbc_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_rsa_aes_256_gcm_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exp_rsa_descbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exp_rsa_rc2_md5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exp_rsa_rc4_md5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_3des_ede_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_aes_128_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_aes_128_cbc_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_aes_256_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_aes_256_cbc_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_des_cbc_sha</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_rc4_128_md5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_rc4_128_sha }</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• In FIPS mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>prefer-cipher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>{ ecdhe_ecdsa_aes_128_cbc_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_ecdsa_aes_128_gcm_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_ecdsa_aes_256_cbc_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_ecdsa_aes_256_gcm_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_rsa_aes_128_cbc_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_rsa_aes_128_gcm_sha256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_rsa_aes_256_cbc_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ecdhe_rsa_aes_256_gcm_sha384</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rsa_aes_128_cbc_sha }</td>
<td></td>
</tr>
</tbody>
</table>
6. Specify the SSL protocol version for the SSL client policy.

In Release 1111:
- In non-FIPS mode:
  version { ssl3.0 | tls1.0 }
- In FIPS mode:
  version tls1.0

In Release 1121 and later:
- In non-FIPS mode:
  version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 }
- In FIPS mode:
  version { tls1.0 | tls1.1 | tls1.2 }

By default, an SSL client policy uses TLS 1.0.
To ensure security, do not specify SSL 3.0 for an SSL client policy.

7. Enable the SSL client to authenticate servers through digital certificates.

server-verify enable

By default, SSL server authentication is enabled.

---

### Displaying and maintaining SSL

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display cryptographic library version information. (Available in Release 1121 and later.)</td>
<td><code>display crypto version</code></td>
</tr>
<tr>
<td>Display SSL server policy information.</td>
<td><code>display ssl server-policy [ policy-name ]</code></td>
</tr>
<tr>
<td>Display SSL client policy information.</td>
<td><code>display ssl client-policy [ policy-name ]</code></td>
</tr>
</tbody>
</table>
Configuring IP source guard

Overview

IP source guard (IPSG) prevents spoofing attacks by using an IPSG binding table to match legitimate packets. It drops packets that do not match the table. IPSG is a per-interface packet filter. Configuring the feature on one interface does not affect packet forwarding on another interface.

The IPSG binding table can include global and interface-specific bindings. IPSG first uses the interface-specific bindings to match packets. If no match is found, IPSG uses the global bindings. The bindings fall into the following types:

- IP
- MAC
- IP-MAC
- IP-VLAN
- MAC-VLAN
- IP-MAC-VLAN

IPSG bindings can be static or dynamic.

- **Static bindings**—Configured manually. Global IPSG supports only static IP-MAC bindings. For more information about global static IPSG bindings, see "Static IPSG bindings."
- **Dynamic bindings**—Generated based on information from other modules. For more information about dynamic bindings, see "Dynamic IPSG bindings."

As shown in Figure 116, IPSG forwards only the packets that match an IPSG binding.

Figure 116 Diagram for the IPSG feature

Static IPSG bindings

Static IPSG bindings are configured manually. They are suitable for scenarios where few hosts exist on a LAN and their IP addresses are manually configured. For example, you can configure a static IPSG binding on an interface that connects to a server. This binding allows the interface to receive packets only from the server.

Static IPSG bindings on an interface implement the following functions:

- Filter incoming IPv4 or IPv6 packets on the interface.
- Cooperate with ARP detection in IPv4 for user validity checking.

For information about ARP detection, see "Configuring ARP attack protection."

Static IPSG bindings can be global or interface-specific.
• **Global static binding**—Binds the IP address and MAC address in system view. The binding takes effect on all interfaces to filter packets for user spoofing attack prevention.

• **Interface-specific static binding**—Binds the IP address, MAC address, VLAN, or any combination of the items in interface view. The binding takes effect only on the interface to check the validity of users who are attempting to access the interface.

**Dynamic IPSG bindings**

IPSG automatically obtains user information from other modules to generate dynamic bindings. The source modules include DHCP relay agent, DHCP snooping, DHCPv6 snooping, and DHCP server.

DHCP-based IPSG bindings are suitable for scenarios where hosts on a LAN obtain IP addresses through DHCP. IPSG is configured on the DHCP snooping device or the DHCP relay agent. It generates dynamic IPSG bindings based on the DHCP snooping entries or DHCP relay entries. IPSG allows only packets from the DHCP clients to pass through.

**Dynamic IPv4SG**

Dynamic bindings generated based on different source modules are for different usages:

<table>
<thead>
<tr>
<th>Interface types</th>
<th>Source modules</th>
<th>Binding usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Ethernet port</td>
<td>DHCP snooping</td>
<td>Packet filtering.</td>
</tr>
<tr>
<td>Layer 3 Ethernet interface/Layer 3 aggregate interface/VLAN interface</td>
<td>DHCP relay agent</td>
<td>Packet filtering.</td>
</tr>
<tr>
<td></td>
<td>DHCP server</td>
<td>For cooperation with modules (such as the ARP detection module) to provide security services.</td>
</tr>
</tbody>
</table>

For information about DHCP snooping, DHCP relay agent, and DHCP server see *Layer 3—IP Services Configuration Guide*.

**Dynamic IPv6SG**

IPv6SG on an interface obtains information from DHCPv6 snooping entries to generate bindings for packet filtering.

For more information about DHCPv6 snooping, see *Layer 3—IP Services Configuration Guide*.

**NOTE:**
The switch supports only dynamic IPv4SG in the current release.

**IPSG configuration task list**

To configure IPv4SG, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) <strong>Enabling IPv4SG on an interface</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional.) <strong>Configuring a static IPv4SG binding</strong></td>
<td></td>
</tr>
</tbody>
</table>

To configure IPv6SG, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) <strong>Enabling IPv6SG on an interface</strong></td>
<td></td>
</tr>
</tbody>
</table>
Configuring the IPv4SG feature

You cannot configure the IPv4SG feature on a service loopback interface. If IPv4SG is enabled on an interface, you cannot assign the interface to a service loopback group.

Enabling IPv4SG on an interface

When you enable IPSG on an interface, the static and dynamic IPSG are both enabled.
- Static IPv4SG uses static bindings configured by using the `ip source binding` command.
- Dynamic IPv4SG generates dynamic bindings from related source modules. IPv4SG uses the bindings to filter incoming IPv4 packets based on the matching criteria specified in the `ip verify source` command.

To implement dynamic IPv4SG, make sure the DHCP snooping or DHCP relay agent feature operates correctly on the network.

To enable the IPv4SG feature on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2.   | interface interface-number | The following interface types are supported:  
  • Layer 2 Ethernet interface.  
  • Layer 3 Ethernet interface.  
  • VLAN interface.  
  • Layer 3 aggregate interface. |
| 3.   | ip verify source { ip-address | ip-address mac-address | mac-address } | By default, the IPv4SG feature is disabled on an interface.  
If you configure this command on an interface multiple times, the most recent configuration takes effect. |

Configuring a static IPv4SG binding

You can configure global static and interface-specific static IPv4SG bindings.

Global static bindings take effect on all interfaces.

Interface-specific static bindings take priority over global static bindings. An interface first uses the static bindings on the interface to match packets. If no match is found, the interface uses the global bindings.

Configuring a global static IPv4SG binding

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ip source binding ip-address ip-address</td>
<td>No global static IPv4SG</td>
</tr>
</tbody>
</table>
Configuring a static IPv4SG binding on an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter interface view. | `interface interface-type interface-number` | The following interface types are supported:  
  - Layer 2 Ethernet interface.  
  - Layer 3 Ethernet interface.  
  - VLAN interface. |
| 3. Configure a static IPv4SG binding. | `ip source binding { ip-address ip-address | ip-address mac-address | mac-address mac-address } [ vlan vlan-id ]` | By default, no static IPv4SG binding is configured on an interface.  
  Support for the `mac-address` and `vlan` keywords depends on the device model.  
  The `vlan vlan-id` option is supported only in Layer 2 Ethernet interface view.  
  To configure a static IPv4SG binding for the ARP detection function, the `vlan vlan-id` option must be specified, and ARP detection must be enabled for the specified VLAN.  
  You can configure the same static IPv4SG binding on different interfaces. |

Configuring the IPv6SG feature

You cannot configure the IPv6SG feature on a service loopback interface. If IPv6SG is enabled on an interface, you cannot assign the interface to a service loopback group.

Enabling IPv6SG on an interface

When you enable IPv6SG on an interface, the static and dynamic IPv6SG are both enabled.
- Static IPv6SG uses static bindings configured by using the `ipv6 source binding` command.
- Dynamic IPv6SG generates dynamic bindings from related source modules. IPv6SG uses the bindings to filter incoming IPv6 packets based on the matching criteria specified in the `ipv6 verify source` command.

To implement dynamic IPv6SG, make sure DHCPv6 snooping operates correctly on the network.
To enable the IPv6SG feature on an interface:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter interface view. | `interface interface-type interface-number` | The following interface types are supported:  
  - Layer 2 Ethernet interface.  
  - Layer 3 Ethernet interface.  
  - VLAN interface. |
3. Enable the IPv6SG feature.

```
ipv6 verify source { ip-address | ip-address mac-address | mac-address }
```

By default, the IPv6SG feature is disabled on an interface.
If you configure this command on an interface multiple times, the most recent configuration takes effect.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Configure a global static IPv6SG binding.</td>
<td>ipv6 source binding ip-address ipv6-address mac-address</td>
<td>No global static IPv6SG binding exists.</td>
</tr>
</tbody>
</table>

### Configuring a static IPv6SG binding

You can configure global static and interface-specific static IPv6SG bindings.

Global static bindings take effect on all interfaces.
Interface-specific static bindings take priority over global static bindings. An interface first uses the static bindings on the interface to match packets. If no match is found, the interface uses the global bindings.

#### Configuring a global static IPv6SG binding

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Configure a global static IPv6SG binding.</td>
<td>ipv6 source binding ip-address ipv6-address mac-address</td>
<td>No global static IPv6SG binding exists.</td>
</tr>
</tbody>
</table>

#### Configuring a static IPv6SG binding on an interface

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter interface view. | interface interface-type interface-number | The following interface types are supported:  
  • Layer 2 Ethernet interface.  
  • Layer 3 Ethernet interface.  
  • VLAN interface. |
| 3. Configure a static IPv6SG binding. | ipv6 source binding { ip-address ipv6-address | ip-address ipv6-address | mac-address mac-address | mac-address mac-address | [ vlan vlan-id ] } | By default, no static IPv6SG binding is configured on an interface. Support for the mac-address and vlan keywords depends on the device model. The vlan vlan-id option is supported only in Layer 2 Ethernet interface view. To configure a static IPv6SG binding for the ND detection function, the vlan vlan-id option must be specified, and ND detection must be enabled for the specified VLAN. You can configure the same static IPv6SG binding on different interfaces. |
Displaying and maintaining IPSG

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display IPv4SG bindings.</td>
<td>`display ip source binding [ static</td>
</tr>
<tr>
<td>Display IPv6SG bindings.</td>
<td>`display ipv6 source binding [ static</td>
</tr>
</tbody>
</table>

IPSG configuration examples

Static IPv4SG configuration example

Network requirements

As shown in Figure 117, all hosts use static IP addresses.

Configure static IPv4SG bindings on Switch A and Switch B to meet the following requirements:

- GigabitEthernet 1/0/2 of Switch A allows only IP packets from Host C to pass.
- GigabitEthernet 1/0/1 of Switch A allows only IP packets from Host A to pass.
- All interfaces of Switch B allow IP packets from Host A to pass.
- GigabitEthernet 1/0/1 of Switch B allows IP packets from Host B to pass.

Figure 117 Network diagram

Configuration procedure

1. Configure Switch A:
   # Configure IP addresses for the interfaces. (Details not shown.)
   # Enable IPv4SG on GigabitEthernet 1/0/2.
   `<SwitchA> system-view`
   `[SwitchA] interface gigabitethernet 1/0/2`
   `[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address`
   # On GigabitEthernet 1/0/2, configure a static IPv4SG binding for Host C.
Verifying the configuration

# Verify that the static IPv4SG bindings are configured successfully on Switch A.
<SwitchA> display ip source binding static
Total entries found: 2
IP Address   MAC Address   Interface         VLAN Type
192.168.0.1   0001-0203-0405 GE1/0/2       N/A  Static
192.168.0.3   0001-0203-0406 GE1/0/1       N/A  Static

# Verify that the static IPv4SG bindings are configured successfully on Device B.
<SwitchB> display ip source binding static
Total entries found: 2
IP Address   MAC Address   Interface         VLAN Type
192.168.0.1   0001-0203-0406 N/A            N/A  Static
N/A           0001-0203-0407 GE1/0/1       N/A  Static

Dynamic IPv4SG using DHCP snooping configuration example

Network requirements

As shown in Figure 118, the host (the DHCP client) obtains an IP address from the DHCP server. Perform the following tasks:
• Enable DHCP snooping on the switch to make sure the DHCP client obtains an IP address from the authorized DHCP server. To generate a DHCP snooping entry for the DHCP client, enable recording of client information in DHCP snooping entries.

• Enable dynamic IPv4SG on GigabitEthernet 1/0/1 to filter incoming packets by using the IPv4SG bindings generated based on DHCP snooping entries. Only packets from the DHCP client are allowed to pass.

Figure 118 Network diagram

Configuration procedure

1. Configure the DHCP server.
   For information about DHCP server configuration, see Layer 3—IP Services Configuration Guide.

2. Configure the switch:
   # Configure IP addresses for the interfaces. (Details not shown.)
   # Enable DHCP snooping.
   <Switch> system-view
   [Switch] dhcp snooping enable
   # Configure GigabitEthernet 1/0/2 as a trusted interface.
   [Switch] interface gigabitethernet 1/0/2
   [Switch-GigabitEthernet1/0/2] dhcp snooping trust
   [Switch-GigabitEthernet1/0/2] quit
   # Enable IPv4SG on GigabitEthernet 1/0/1 and verify the source IP address and MAC address for dynamic IPSG.
   [Switch] interface gigabitethernet 1/0/1
   [Switch-GigabitEthernet1/0/1] ip verify source ip-address mac-address
   # Enable recording of client information in DHCP snooping entries on GigabitEthernet 1/0/1.
   [Switch-GigabitEthernet1/0/1] dhcp snooping binding record
   [Switch-GigabitEthernet1/0/1] quit

Verifying the configuration

# Verify that a dynamic IPv4SG binding is generated based on a DHCP snooping entry
[Switch] display ip source binding dhcp-snooping
Total entries found: 1
IP Address      MAC Address    Interface                VLAN Type
192.168.0.1     0001-0203-0406 GE1/0/1                   1    DHCP snooping

Dynamic IPv4SG using DHCP relay agent configuration example

Network requirements

As shown in Figure 119, DHCP relay agent is enabled on the switch. The host obtains an IP address from the DHCP server through the DHCP relay agent.
Enable dynamic IPv4SG on VLAN-interface 100 to filter incoming packets by using the IPv4SG bindings generated based on DHCP relay entries.

**Figure 119 Network diagram**

```
DHCP client         DHCP relay agent     DHCP server

Host
MAC: 0001-0203-0406

Switch
Vlan-int100
Vlan-int200

10.1.1.1/24
```

**Configuration procedure**

1. **Configure dynamic IPv4SG:**
   
   ```
   # Configure IP addresses for the interfaces. (Details not shown.)
   # Enable IPv4SG on VLAN-interface 100 and verify the source IP address and MAC address for dynamic IPSG.
   <Switch> system-view
   [Switch] interface vlan-interface 100
   [Switch-Vlan-interface100] ip verify source ip-address mac-address
   [Switch-Vlan-interface100] quit
   ```

2. **Configure the DHCP relay agent:**
   
   ```
   # Enable the DHCP service.
   [Switch] dhcp enable
   # Enable recording DHCP relay client entries.
   [Switch] dhcp relay client-information record
   # Configure VLAN-interface 100 to operate in DHCP relay mode.
   [Switch] interface vlan-interface 100
   [Switch-Vlan-interface100] dhcp select relay
   # Specify the IP address of the DHCP server.
   [Switch-Vlan-interface100] dhcp relay server-address 10.1.1.1
   [Switch-Vlan-interface100] quit
   ```

**Verifying the configuration**

```
# Verify that a dynamic IPv4SG binding is generated based on a DHCP relay entry.
[Switch] display ip source binding dhcp-relay
Total entries found: 1
IP Address    MAC Address    Interface                VLAN Type
192.168.0.1    0001-0203-0406 Vlan100                  100  DHCP relay
```

**Static IPv6SG configuration example**

**Network requirements**

As shown in Figure 120, configure a static IPv6SG binding for GigabitEthernet 1/0/1 of the device to allow only IPv6 packets from the host to pass.
Configuration procedure

# Enable IPv6SG on GigabitEthernet 1/0/1.
<Switch> system-view
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address

# On GigabitEthernet 1/0/1, configure a static IPv6SG binding for the host.
[Switch-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address 0001-0202-0202
[Switch-GigabitEthernet1/0/1] quit

Verifying the configuration

# Verify that the static IPv6SG binding is configured successfully on the switch.
[Switch] display ipv6 source binding static
Total entries found: 1
IPv6 Address         MAC Address    Interface               VLAN Type
2001::1              0001-0202-0202 GE1/0/1                  N/A  Static

Dynamic IPv6SG using DHCPv6 snooping configuration example

Network requirements

As shown in Figure 121, the host (the DHCPv6 client) obtains an IP address from the DHCPv6 server. Perform the following tasks:

- Enable DHCPv6 snooping on the switch to make sure the DHCPv6 client obtains an IPv6 address from the authorized DHCPv6 server. To generate a DHCPv6 snooping entry for the DHCPv6 client, enable recording of client information in DHCPv6 snooping entries.
- Enable dynamic IPv6SG on GigabitEthernet 1/0/1 to filter incoming packets by using the IPv6SG bindings generated based on DHCPv6 snooping entries. Only packets from the DHCPv6 client are allowed to pass.

Configuration procedure

1. Configure DHCPv6 snooping:
   # Enable DHCPv6 snooping globally.
   <Switch> system-view
   [Switch] ipv6 dhcp snooping enable
# Configure the interface connecting to the DHCP server as a trusted interface.
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] ipv6 dhcp snooping trust
[Switch-GigabitEthernet1/0/2] quit

2. Enable IPv6SG:

   # Enable IPv6SG on GigabitEthernet 1/0/1 and verify the source IP address and MAC address for dynamic IPv6SG.
   [Switch] interface gigabitethernet 1/0/1
   [Switch-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address

   # Enable recording of client information in DHCPv6 snooping entries on GigabitEthernet 1/0/1.
   [Switch-GigabitEthernet1/0/1] ipv6 dhcp snooping binding record
   [Switch-GigabitEthernet1/0/1] quit

Verifying the configuration

   # Verify that a dynamic IPv6SG binding is generated based on a DHCPv6 snooping entry.
   [Switch] display ipv6 source binding dhcpv6-snooping
   Total entries found: 1

<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>MAC Address</th>
<th>Interface</th>
<th>VLAN Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::1</td>
<td>040a-0000-0001</td>
<td>GE1/0/1</td>
<td>1 DHCPv6 snooping</td>
</tr>
</tbody>
</table>
Configuring ARP attack protection

ARP attacks and viruses are threatening LAN security. This chapter describes multiple features used to detect and prevent ARP attacks.

Although ARP is easy to implement, it provides no security mechanism and is vulnerable to network attacks. An attacker can exploit ARP vulnerabilities to attack network devices in the following ways:

- Acts as a trusted user or gateway to send ARP packets so the receiving devices obtain incorrect ARP entries.
- Sends a large number of unresolvable IP packets to have the receiving device busy with resolving IP addresses until its CPU is overloaded. Unresolvable IP packets refer to IP packets for which ARP cannot find corresponding MAC addresses.
- Sends a large number of ARP packets to overload the CPU of the receiving device.

For more information about ARP attack features and types, see *ARP Attack Protection Technology White Paper*.

### ARP attack protection configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flood prevention:</strong></td>
</tr>
<tr>
<td>- Configuring unresolvable IP attack protection (configured on gateways)</td>
</tr>
<tr>
<td>- Configuring ARP source suppression</td>
</tr>
<tr>
<td>- Configuring ARP blackhole routing</td>
</tr>
<tr>
<td>- Configuring ARP packet rate limit (configured on access devices)</td>
</tr>
<tr>
<td>- Configuring source MAC-based ARP attack detection (configured on gateways)</td>
</tr>
<tr>
<td><strong>User and gateway spoofing prevention:</strong></td>
</tr>
<tr>
<td>- Configuring ARP packet source MAC consistency check (configured on gateways)</td>
</tr>
<tr>
<td>- Configuring ARP active acknowledgement (configured on gateways)</td>
</tr>
<tr>
<td>- Configuring authorized ARP (configured on gateways)</td>
</tr>
<tr>
<td>- Configuring ARP attack detection (configured on access devices)</td>
</tr>
<tr>
<td>- Configuring ARP scanning and fixed ARP (configured on gateways)</td>
</tr>
<tr>
<td>- Configuring ARP gateway protection (configured on access devices)</td>
</tr>
<tr>
<td>- Configuring ARP filtering (configured on access devices)</td>
</tr>
</tbody>
</table>

### Configuring unresolvable IP attack protection

If a device receives a large number of unresolvable IP packets from a host, the following situations can occur:

- The device sends a large number of ARP requests, overloading the target subnets.
- The device keeps trying to resolve target IP addresses, overloading its CPU.

To protect the device from such IP attacks, you can configure the following features:

- **ARP source suppression**—stops resolving packets from a host if the number of unresolvable IP packets from the host exceeds the upper limit within 5 seconds. The device continues ARP resolution when the interval elapses. This feature is applicable if the attack packets have the same source addresses.
- **ARP blackhole routing**—Creates a blackhole route destined for an unresolved IP address. The device drops all matching packets until the blackhole route is deleted. A blackhole route is deleted when its aging timer (25 seconds) is reached or the route becomes reachable.

After a blackhole route is created for an unresolved IP address, the device immediately starts the first ARP blackhole route probe by sending an ARP request. If the resolution fails, the device continues probing according to the probe settings. If the IP address resolution succeeds in a probe, the device converts the blackhole route to a normal route. If an ARP blackhole route ages out before the device finishes all probes, the device deletes the blackhole route and does not perform the remaining probes.

This feature is applicable regardless of whether the attack packets have the same source addresses.

### Configuring ARP source suppression

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>arp source-suppression enable</td>
<td>By default, ARP source suppression is disabled.</td>
</tr>
<tr>
<td>3.</td>
<td>arp source-suppression limit limit-value</td>
<td>By default, the maximum number is 10.</td>
</tr>
</tbody>
</table>

### Configuring ARP blackhole routing

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>arp resolving-route enable</td>
<td>By default, ARP blackhole routing is enabled.</td>
</tr>
<tr>
<td>3.</td>
<td>arp resolving-route probe-interval interval</td>
<td>The default setting is 1 second.</td>
</tr>
<tr>
<td>4.</td>
<td>arp resolving-route probe-count count</td>
<td>The default setting is one probe.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining unresolvable IP attack protection

Execute **display** commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display ARP source suppression configuration information.</td>
<td>display arp source-suppression</td>
</tr>
</tbody>
</table>
Configuration example

Network requirements

As shown in Figure 122, a LAN contains two areas: an R&D area in VLAN 10 and an office area in VLAN 20. Each area connects to the gateway (Device) through an access switch.

A large number of ARP requests are detected in the office area and are considered as the consequence of an unresolvable IP attack. To prevent the attack, configure ARP source suppression or ARP blackhole routing.

Figure 122 Network diagram

---

Configuration procedure

- If the attack packets have the same source address, configure ARP source suppression:
  
  ```
  # Enable ARP source suppression.
  <Device> system-view
  [Device] arp source-suppression enable
  # Allow the device to receive a maximum of 100 unresolvable packets from a host in 5 seconds.
  [Device] arp source-suppression limit 100
  ```

- If the attack packets have different source addresses, configure ARP blackhole routing:
  
  ```
  # Enable ARP blackhole routing.
  [Device] arp resolving-route enable
  ```

---

Configuring ARP packet rate limit

The ARP packet rate limit feature allows you to limit the rate of ARP packets delivered to the CPU. An ARP attack detection-enabled device will send all received ARP packets to the CPU for inspection. Processing excessive ARP packets will make the device malfunction or even crash. To solve this problem, configure ARP packet rate limit.
Configuration guidelines

Configure this feature when MFF, ARP attack detection, or ARP snooping is enabled, or when ARP flood attacks are detected.

Configuration procedure

This task sets a rate limit for ARP packets received on an interface. When the number of ARP packets that the interface receives within a period exceeds the rate limit, those packets are discarded.

You can enable sending of notifications to the SNMP module or enable logging for ARP packet rate limit.

- If notification sending is enabled, the device sends the highest threshold-crossed ARP packet rate within the sending interval in a notification to the SNMP module. You must use the `snmp-agent target-host` command to set the notification type and target host. For more information about notifications, see Network Management and Monitoring Command Reference.

- If logging for ARP packet rate limit is enabled, the device sends the highest threshold-crossed ARP packet rate within the sending interval in a log message to the information center. You can configure the information center module to set the log output rules. For more information about information center, see Network Management and Monitoring Configuration Guide.

To configure ARP packet rate limit:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Enable notification sending for ARP packet rate limit.</td>
<td><code>snmp-agent trap enable arp [ rate-limit ]</code></td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Enable logging for ARP packet rate limit.</td>
<td><code>arp rate-limit log enable</code></td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Set the notification and log message sending interval.</td>
<td><code>arp rate-limit log interval seconds</code></td>
</tr>
<tr>
<td>5.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>6.</td>
<td>Enable ARP packet rate limit and set the rate limit.</td>
<td><code>arp rate-limit [ pps ]</code></td>
</tr>
</tbody>
</table>

**NOTE:**

If you enable notification sending and logging for ARP packet rate limit on a Layer 2 aggregate interface, the features apply to all aggregation member ports.

Configuring source MAC-based ARP attack detection

This feature checks the number of ARP packets delivered to the CPU. If the number of packets from the same MAC address within 5 seconds exceeds a threshold, the device adds the MAC address to
an ARP attack entry. Before the entry is aged out, the device handles the attack by using either of the following methods:

- **Monitor**—Only generates log messages.
- **Filter**—Generates log messages and filters out subsequent ARP packets from that MAC address.

You can exclude the MAC addresses of some gateways and servers from this detection. This feature does not inspect ARP packets from those devices even if they are attackers.

**Configuration procedure**

To configure source MAC-based ARP attack detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable source MAC-based ARP attack detection and specify the handling method.</td>
<td>`arp source-mac { filter</td>
</tr>
<tr>
<td>3.</td>
<td>Set the threshold.</td>
<td><code>arp source-mac threshold threshold-value</code></td>
</tr>
<tr>
<td>4.</td>
<td>Set the aging timer for ARP attack entries.</td>
<td><code>arp source-mac aging-time time</code></td>
</tr>
<tr>
<td>5.</td>
<td>(Optional.) Exclude specific MAC addresses from this detection.</td>
<td><code>arp source-mac exclude-mac mac-address&lt;&amp;1-10&gt;</code></td>
</tr>
</tbody>
</table>

**NOTE:**

When an ARP attack entry is aged out, ARP packets sourced from the MAC address in the entry can be processed correctly.

**Displaying and maintaining source MAC-based ARP attack detection**

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display ARP attack entries detected by source MAC-based ARP attack detection.</td>
<td>`display arp source-mac { slot slot-number</td>
</tr>
</tbody>
</table>

**Configuration example**

**Network requirements**

As shown in Figure 123, the hosts access the Internet through a gateway (Device). If malicious users send a large number of ARP requests to the gateway, the gateway might crash and cannot process requests from the clients. To solve this problem, configure source MAC-based ARP attack detection on the gateway.
Configuration considerations

An attacker might forge a large number of ARP packets by using the MAC address of a valid host as the source MAC address. To prevent such attacks, configure the gateway in the following steps:

1. Enable source MAC-based ARP attack detection and specify the handling method as filter.
2. Set the threshold.
3. Set the lifetime for ARP attack entries.
4. Exclude the MAC address of the server from this detection.

Configuration procedure

# Enable source MAC-based ARP attack detection, and specify the handling method as filter.
<Device> system-view
[Device] arp source-mac filter
# Set the threshold to 30.
[Device] arp source-mac threshold 30
# Set the lifetime for ARP attack entries to 60 seconds.
[Device] arp source-mac aging-time 60
# Exclude MAC address 0012-3f86-e94c from this detection.
[Device] arp source-mac exclude-mac 0012-3f86-e94c

Configuring ARP packet source MAC consistency check

This feature enables a gateway to filter out ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body. This feature allows the gateway to learn correct ARP entries.

To enable ARP packet source MAC address consistency check:
### Configuring ARP active acknowledgement

Configure this feature on gateways to prevent user spoofing.

ARP active acknowledgement prevents a gateway from generating incorrect ARP entries.

In strict mode, a gateway performs more strict validity checks before creating an ARP entry:
- Upon receiving an ARP request destined for the gateway, the gateway sends an ARP reply but does not create an ARP entry.
- Upon receiving an ARP reply, the gateway determines whether it has resolved the sender IP address:
  - If yes, the gateway performs active acknowledgement. When the ARP reply is verified as valid, the gateway creates an ARP entry.
  - If no, the gateway discards the packet.

To configure ARP active acknowledgement:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable the ARP active acknowledgement feature.</td>
<td>arp active-ack [ strict ] enable</td>
<td>By default, this feature is disabled.</td>
</tr>
</tbody>
</table>

### Configuring authorized ARP

Authorized ARP entries are generated based on the DHCP clients’ address leases on the DHCP server or dynamic client entries on the DHCP relay agent. For more information about DHCP server and DHCP relay agent, see *Layer 3—IP Services Configuration Guide*.

With authorized ARP enabled, an interface is disabled from learning dynamic ARP entries. This feature prevents user spoofing and allows only authorized clients to access network resources.

**Configuration procedure**

To enable authorized ARP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter interface view. | interface interface-type interface-number | The device supports the following interface types:
  - Layer 3 Ethernet interface.
  - Layer 3 aggregate interface.
  - VLAN interface. |
### Configuration example (on a DHCP server)

#### Network requirements

As shown in Figure 124, configure authorized ARP on GigabitEthernet 1/0/1 of Switch A (a DHCP server) to ensure user validity.

**Figure 124 Network diagram**

Switch A Switch B

GE1/0/1 10.1.1.1/24

#### Configuration procedure

1. **Configure Switch A:**
   
   ```
   # Specify the IP address for GigabitEthernet 1/0/1.
   <SwitchA> system-view
   [SwitchA] interface gigabitethernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] port link-mode route
   [SwitchA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
   [SwitchA-GigabitEthernet1/0/1] quit
   # Configure DHCP.
   [SwitchA] dhcp enable
   [SwitchA] dhcp server ip-pool 1
   [SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
   [SwitchA-dhcp-pool-1] quit
   # Enter Layer 3 Ethernet interface view.
   [SwitchA] interface gigabitethernet 1/0/1
   # Enable authorized ARP.
   [SwitchA-GigabitEthernet1/0/1] arp authorized enable
   [SwitchA-GigabitEthernet1/0/1] quit
   ```

2. **Configure Switch B:**

   ```
   <SwitchB> system-view
   [SwitchB] interface gigabitethernet 1/0/1
   [SwitchB-GigabitEthernet1/0/1] port link-mode route
   [SwitchB-GigabitEthernet1/0/1] ip address dhcp-alloc
   [SwitchB-GigabitEthernet1/0/1] quit
   ```

#### Verifying the configuration

```
# Display authorized ARP entry information on Switch A.
[SwitchA] display arp all

<table>
<thead>
<tr>
<th>Type</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>VLAN</th>
<th>Interface</th>
<th>Aging</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-Static</td>
<td>10.1.1.2</td>
<td>0012-3f86-e94c</td>
<td>N/A</td>
<td>GE1/0/1</td>
<td>20</td>
<td>D</td>
</tr>
</tbody>
</table>
```
The output shows that IP address 10.1.1.2 has been assigned to Switch B. Switch B must use the IP address and MAC address in the authorized ARP entry to communicate with Switch A. Otherwise, the communication fails. Thus user validity is ensured.

Configuration example (on a DHCP relay agent)

Network requirements

As shown in Figure 125, configure authorized ARP on GigabitEthernet 1/0/2 of Switch B (a DHCP relay agent) to ensure user validity.

Figure 125 Network diagram

Configuration procedure

1. Configure Switch A:
   # Specify the IP address for GigabitEthernet 1/0/1.
   <SwitchA> system-view
   [SwitchA] interface gigabitethernet 1/0/1
   [SwitchA-GigabitEthernet1/0/1] port link-mode route
   [SwitchA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
   [SwitchA-GigabitEthernet1/0/1] quit
   # Configure DHCP.
   [SwitchA] dhcp enable
   [SwitchA] dhcp server ip-pool 1
   [SwitchA-dhcp-pool-1] network 10.10.1.0 mask 255.255.255.0
   [SwitchA-dhcp-pool-1] gateway-list 10.10.1.1
   [SwitchA-dhcp-pool-1] quit
   [SwitchA] ip route-static 10.10.1.0 24 10.1.1.2

2. Configure Switch B:
   # Enable DHCP.
   <SwitchB> system-view
   [SwitchB] dhcp enable
   # Specify the IP addresses of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.
   [SwitchB] interface gigabitethernet 1/0/1
   [SwitchB-GigabitEthernet1/0/1] port link-mode route
   [SwitchB-GigabitEthernet1/0/1] ip address 10.1.1.2 24
   [SwitchB-GigabitEthernet1/0/1] quit
   [SwitchB] interface gigabitethernet 1/0/2
   [SwitchB-GigabitEthernet1/0/2] port link-mode route
   [SwitchB-GigabitEthernet1/0/2] ip address 10.10.1.1 24
# Enable DHCP relay agent on GigabitEthernet 1/0/2.
[SwitchB-GigabitEthernet1/0/2] dhcp select relay

# Add the DHCP server 10.1.1.1 to DHCP server group 1.
[SwitchB-GigabitEthernet1/0/2] dhcp relay server-address 10.1.1.1

# Enable authorized ARP.
[SwitchB-GigabitEthernet1/0/2] arp authorized enable
[SwitchB-GigabitEthernet1/0/2] quit

# Enable recording of relay entries on the relay agent.
[SwitchB] dhcp relay client-information record

3. Configure Switch C:

<SwitchC> system-view
[SwitchC] ip route-static 10.1.1.0 24 10.10.1.1
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-mode route
[SwitchC-GigabitEthernet1/0/2] ip address dhcp-alloc
[SwitchC-GigabitEthernet1/0/2] quit

Verifying the configuration

# Display authorized ARP information on Switch B.
[SwitchB] display arp all

| Type: S-Static   D-Dynamic   O-Openflow   M-Multiport I-Invalid |
|-----------------|-----------------|-----------------|-----------------|-----------------|
| IP Address      | MAC Address     | VLAN | Interface | Aging Type     |
| 10.10.1.2       | 0012-3f86-e94c  | N/A  | GE1/0/2   | 20 D           |

The output shows that Switch A assigned the IP address 10.10.1.2 to Switch C.
Switch C must use the IP address and MAC address in the authorized ARP entry to communicate with Switch B. Otherwise, the communication fails. Thus the user validity is ensured.

Configuring ARP attack detection

ARP attack detection enables access devices to block ARP packets from unauthorized clients to prevent user spoofing and gateway spoofing attacks. ARP attack detection does not check ARP packets received from ARP trusted ports.

ARP attack detection provides the following features:

- User validity check.
- ARP packet validity check.
- ARP restricted forwarding.
- ARP attack detection logging.

If both ARP packet validity check and user validity check are enabled, the former one applies first, and then the latter applies.

Configuring user validity check

Upon receiving an ARP packet from an ARP untrusted interface, the device matches the sender IP and MAC addresses with the following entries:

- Static IP source guard bindings
- DHCP snooping entries
If a match is found, the ARP packet is considered valid and is forwarded. If no match is found, the ARP packet is considered invalid and is discarded.

Static IP source guard bindings are created by using the `ip source binding` command. For more information, see "Configuring IP source guard."

DHCP snooping entries are automatically generated by DHCP snooping. For more information, see *Layer 3—IP Services Configuration Guide*.

**Configuration guidelines**

When you configure user validity check, follow these guidelines:

- Make sure at least one among static IP source guard bindings, and DHCP snooping entries is configured for user validity check. Otherwise, ARP packets received from ARP untrusted ports are discarded.
- You must specify a VLAN for an IP source guard binding. Otherwise, no ARP packets can match the IP source guard binding.

**Configuration procedure**

To configure user validity check:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter VLAN view.</td>
<td><code>vlan vlan-id</code></td>
</tr>
<tr>
<td>3.</td>
<td>Enable ARP attack detection.</td>
<td><code>arp detection enable</code></td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
<td><code>quit</code></td>
</tr>
<tr>
<td>5.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td><code>interface interface-type interface-number</code></td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Configure the interface as a trusted interface excluded from ARP attack detection.</td>
<td><code>arp detection trust</code></td>
</tr>
</tbody>
</table>

**Configuring ARP packet validity check**

Enable validity check for ARP packets received on untrusted ports and specify the following objects to be checked:

- **src-mac**—Checks whether the sender MAC address in the message body is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded. Otherwise, the packet is discarded.
- **dst-mac**—Checks the target MAC address of ARP replies. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.
- **ip**—Checks the sender and target IP addresses of ARP replies, and the sender IP address of ARP requests. all-one, or multicast IP addresses are considered invalid and the corresponding packets are discarded.

To configure ARP packet validity check:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
</tbody>
</table>

421
### Configuring ARP restricted forwarding

**NOTE:**
ARP restricted forwarding does not apply to ARP packets with multiport MAC as their destination MAC addresses.

ARP restricted forwarding controls the forwarding of ARP packets that are received on untrusted interfaces and have passed user validity check as follows:

- If the packets are ARP requests, they are forwarded through the trusted interface.
- If the packets are ARP replies, they are forwarded according to their destination MAC address. If no match is found in the MAC address table, they are forwarded through the trusted interface.

Configure user validity check before you configure ARP restricted forwarding.

To enable ARP restricted forwarding:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>vlan vlan-id</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>arp restricted-forwarding enable</td>
<td>By default, ARP restricted forwarding is disabled.</td>
</tr>
</tbody>
</table>

### Enabling ARP attack detection logging

**IMPORTANT:**
This feature is available in Release 1121 and later.

The ARP attack detection logging feature enables a device to generate ARP attack detection log messages when illegal ARP packets are detected. An ARP attack detection log message contains the following information:

1. Receiving interface of the ARP packets.
2. Sender IP address.
3. Total number of dropped ARP packets.
The following is an example of an ARP attack detection log message:
Detected an inspection occurred on interface GigabitEthernet1/0/1 with IP address 172.18.48.55 (Total 10 packets dropped).

To enable ARP attack detection logging:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable ARP attack detection logging.</td>
<td>arp detection log enable</td>
</tr>
</tbody>
</table>

Displaying and maintaining ARP attack detection

Execute `display` commands in any view and `reset` commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the VLANs enabled with ARP attack detection.</td>
<td><code>display arp detection</code></td>
</tr>
<tr>
<td>Display the ARP attack detection statistics.</td>
<td><code>display arp detection statistics [ interface interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Clear the ARP attack detection statistics.</td>
<td><code>reset arp detection statistics [ interface interface-type interface-number ]</code></td>
</tr>
</tbody>
</table>

User validity check and ARP packet validity check configuration example

**Network requirements**

As shown in Figure 126, configure DHCP snooping on Switch B, and enable ARP attack detection in VLAN 10. Switch B performs ARP packet validity check and user validity check based on static IP source guard bindings and DHCP snooping entries for connected hosts.

**Figure 126 Network diagram**

Switch A

Gateway

DHCP server

GE1/0/3
Vlan-int10
10.1.1.1/24

VLAN 10

DHCP snooping

Switch B

GE1/0/3

GE1/0/1

GE1/0/2

Host A
DHCP client

10.1.1.6
0001-0203-0607

Host B

10.1.1.6

0001-0203-0607
Configuration procedure

1. Add all interfaces on Switch B to VLAN 10, and specify the IP address of VLAN-interface 10 on Switch A. (Details not shown.)
2. Configure the DHCP server on Switch A, and configure DHCP address pool 0.
   ```
   <SwitchA> system-view
   [SwitchA] dhcp enable
   [SwitchA] dhcp server ip-pool 0
   [SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
   ```
3. Configure Host A (DHCP client) and Host B. (Details not shown.)
4. Configure Switch B:
   ```
   # Enable DHCP snooping.
   <SwitchB> system-view
   [SwitchB] dhcp snooping enable
   [SwitchB] interface gigabitethernet 1/0/3
   [SwitchB-GigabitEthernet1/0/3] dhcp snooping trust
   [SwitchB-GigabitEthernet1/0/3] quit
   # Enable recording of client information in DHCP snooping entries on GigabitEthernet 1/0/1.
   [SwitchB] interface gigabitethernet 1/0/1
   [SwitchB-GigabitEthernet1/0/1] dhcp snooping binding record
   [SwitchB-GigabitEthernet1/0/1] quit
   # Enable ARP attack detection for VLAN 10.
   [SwitchB] vlan 10
   [SwitchB-vlan10] arp detection enable
   # Configure the upstream interface as a trusted interface. By default, an interface is an untrusted interface.
   [SwitchB-vlan10] interface gigabitethernet 1/0/3
   [SwitchB-GigabitEthernet1/0/3] arp detection trust
   [SwitchB-GigabitEthernet1/0/3] quit
   # Configure a static IP source guard binding on interface GigabitEthernet 1/0/2 for user validity check.
   [SwitchB] interface gigabitethernet 1/0/2
   [SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address 0001-0203-0607 vlan 10
   [SwitchB-GigabitEthernet1/0/2] quit
   # Enable ARP packet validity check by checking the MAC addresses and IP addresses of ARP packets.
   [SwitchB] arp detection validate dst-mac ip src-mac
   ```
   After the configurations are completed, Switch B first checks the validity of ARP packets received on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. If the ARP packets are confirmed as valid, the switch performs user validity check by using the static IP source guard bindings and finally DHCP snooping entries.

ARP restricted forwarding configuration example

Network requirements

As shown in Figure 127, configure ARP restricted forwarding on Switch B where ARP attack detection is configured. Port isolation configured on Switch B can take effect for broadcast ARP requests.
Figure 127 Network diagram

![Network Diagram]

**Configuration procedure**

1. Configure VLAN 10, add interfaces to VLAN 10, and specify the IP address of the VLAN interface. (Details not shown.)

2. Configure the DHCP server on Switch A, and configure DHCP address pool 0.

   ```
   <SwitchA> system-view
   [SwitchA] dhcp enable
   [SwitchA] dhcp server ip-pool 0
   [SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
   ```

3. Configure Host A (DHCP client) and Host B. (Details not shown.)

4. Configure Switch B:

   ```
   # Enable DHCP snooping, and configure GigabitEthernet 1/0/3 as a DHCP-trusted port.
   <SwitchB> system-view
   [SwitchB] dhcp snooping enable
   [SwitchB] interface gigabitethernet 1/0/3
   [SwitchB-GigabitEthernet1/0/3] dhcp snooping trust
   [SwitchB-GigabitEthernet1/0/3] quit
   
   # Enable ARP attack detection for user validity check.
   [SwitchB] vlan 10
   [SwitchB-vlan10] arp detection enable
   
   # Configure GigabitEthernet 1/0/3 as an ARP-trusted port.
   [SwitchB-vlan10] interface gigabitethernet 1/0/3
   [SwitchB-GigabitEthernet1/0/3] arp detection trust
   [SwitchB-GigabitEthernet1/0/3] quit
   
   # Configure a static IP source guard entry on interface GigabitEthernet 1/0/2.
   [SwitchB] interface gigabitethernet 1/0/2
   [SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address 0001-0203-0607 vlan 10
   [SwitchB-GigabitEthernet1/0/2] quit
   
   # Enable ARP packet validity check by checking the MAC addresses and IP addresses of ARP packets.
   [SwitchB] arp detection validate dst-mac ip src-mac
   ```
# Configure port isolation.

[SwitchB] port-isolate group 1
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port-isolate enable group 1
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port-isolate enable group 1
[SwitchB-GigabitEthernet1/0/2] quit

After the configurations are completed, Switch B first checks the validity of ARP packets received on interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. If the ARP packets are confirmed as valid, the switch performs user validity check by using the static IP source guard bindings and DHCP snooping entries. However, ARP broadcast requests sent from Host A can pass the check on Switch B and reach Host B. Port isolation fails.

# Enable ARP restricted forwarding.

[SwitchB] vlan 10
[SwitchB-vlan10] arp restricted-forwarding enable
[SwitchB-vlan10] quit

After the configuration is completed, Switch B forwards ARP broadcast requests from Host A to Switch A through the trusted interface GigabitEthernet 1/0/3. Host B cannot receive such packets. Port isolation works correctly.

### Configuring ARP scanning and fixed ARP

ARP scanning is typically used together with the fixed ARP feature in small-scale networks.

ARP scanning automatically creates ARP entries for devices in an address range. The device performs ARP scanning in the following steps:

1. Sends ARP requests for each IP address in the address range.
2. Obtains their MAC addresses through received ARP replies.
3. Creates dynamic ARP entries.

Fixed ARP converts existing dynamic ARP entries (including those generated through ARP scanning) to static ARP entries. This feature prevents ARP entries from being modified by attackers. Static ARP entries can also be manually configured by the `arp static` command.

### Configuration restrictions and guidelines

When you configure ARP scanning and fixed ARP, follow these restrictions and guidelines:

- IP addresses in existing ARP entries are not scanned.
- ARP scanning will take some time. To stop an ongoing scan, press Ctrl + C. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.
- The `arp fixup` command is a one-time operation. You can use this command again to convert the dynamic ARP entries learned later to static.
- Due to the limit on the total number of static ARP entries, some dynamic ARP entries might fail the conversion.
- To delete a static ARP entry converted from a dynamic one, use the `undo arp ip-address [ vpn-instance-name ]` command. Use the `reset arp all` command to delete all ARP entries or the `reset arp static` command to delete all static ARP entries.
Configuration procedure

To configure ARP scanning and fixed ARP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 3 Ethernet interface/VLAN interface/Layer 3 aggregate interface view.</td>
</tr>
<tr>
<td>3.</td>
<td>Trigger an ARP scanning.</td>
</tr>
<tr>
<td>4.</td>
<td>Return to system view.</td>
</tr>
<tr>
<td>5.</td>
<td>Enable fixed ARP.</td>
</tr>
</tbody>
</table>

Configuring ARP gateway protection

Configure this feature on interfaces not connected to a gateway to prevent gateway spoofing attacks.

When such an interface receives an ARP packet, it checks whether the sender IP address in the packet is consistent with that of any protected gateway. If yes, it discards the packet. If not, it handles the packet correctly.

Configuration guidelines

Follow these guidelines when you configure ARP gateway protection:

- You can enable ARP gateway protection for a maximum of eight gateways on an interface.
- Do not configure both the arp filter source and arp filter binding commands on an interface.
- If ARP gateway protection works with ARP attack detection, MFF, and ARP snooping, ARP gateway protection applies first.

Configuration procedure

To configure ARP gateway protection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface and Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable ARP gateway protection for the specified gateway.</td>
<td>arp filter source ip-address</td>
</tr>
</tbody>
</table>
Configuration example

Network requirements

As shown in Figure 128, Host B launches gateway spoofing attacks to Switch B. As a result, traffic that Switch B intends to send to Switch A is sent to Host B.

Configure Switch B to block such attacks.

Figure 128 Network diagram

Configuration procedure

# Configure ARP gateway protection on Switch B.
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] arp filter source 10.1.1.1
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] arp filter source 10.1.1.1

Verifying the configuration

# Verify that GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 discard the incoming ARP packets whose sender IP address is the IP address of the gateway.

Configuring ARP filtering

The ARP filtering feature can prevent gateway spoofing and user spoofing attacks.

An interface enabled with this feature checks the sender IP and MAC addresses in a received ARP packet against permitted entries. If a match is found, the packet is handled correctly. If not, the packet is discarded.

Configuration guidelines

Follow these guidelines when you configure ARP filtering:

- You can configure a maximum of eight permitted entries on an interface.
- Do not configure both the arp filter source and arp filter binding commands on an interface.
If ARP filtering works with ARP attack detection, MFF, and ARP snooping, ARP filtering applies first.

Configuration procedure

To configure ARP filtering:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface or Layer 2 aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable ARP filtering and configure a permitted entry.</td>
<td>arp filter binding ip-address mac-address</td>
</tr>
</tbody>
</table>

Configuration example

Network requirements

As shown in Figure 129, the IP and MAC addresses of Host A are 10.1.1.2 and 000f-e349-1233, respectively. The IP and MAC addresses of Host B are 10.1.1.3 and 000f-e349-1234, respectively.

Configure ARP filtering on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch B to permit ARP packets from only Host A and Host B.

Figure 129 Network diagram

<table>
<thead>
<tr>
<th>Configuration procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td># Configure ARP filtering on Switch B.</td>
</tr>
<tr>
<td>&lt;SwitchB&gt; system-view</td>
</tr>
<tr>
<td>[SwitchB] interface gigabitethernet 1/0/1</td>
</tr>
<tr>
<td>[SwitchB-GigabitEthernet1/0/1] arp filter binding 10.1.1.2 000f-e349-1233</td>
</tr>
<tr>
<td>[SwitchB-GigabitEthernet1/0/1] quit</td>
</tr>
<tr>
<td>[SwitchB] interface gigabitethernet 1/0/2</td>
</tr>
<tr>
<td>[SwitchB-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234</td>
</tr>
</tbody>
</table>
Verifying the configuration

# Verify that GigabitEthernet 1/0/1 permits ARP packets from Host A and discards other ARP packets.

# Verify that GigabitEthernet 1/0/2 permits ARP packets from Host B and discards other ARP packets.
Configuring MFF

Overview

MAC-forced forwarding (MFF) implements Layer 2 isolation and Layer 3 communication between hosts in the same broadcast domain.

An MFF enabled device intercepts ARP requests and returns the MAC address of a gateway (or server) to the senders. In this way, the senders are forced to send packets to the gateway for traffic monitoring and attack prevention.

NOTE:
MFF does not support VRRPE for a gateway.

As shown in Figure 130, hosts are connected to Switch C through Switch A and Switch B, which are called Ethernet access nodes (EANs). The MFF enabled EANs forward packets from hosts to the gateway for further forwarding. The hosts are isolated at Layer 2, but they can communicate at Layer 3.

An MFF-enabled device and a host cannot ping each other.

Figure 130 Network diagram for MFF

MFF works with any of the following features to implement traffic filtering and Layer 2 isolation on the EANs:

- ARP snooping (see Layer 3—IP Services Configuration Guide).
- IP source guard (see "Configuring IP source guard").
- ARP detection (see "Configuring ARP attack protection").
- VLAN mapping (see Layer 2—LAN Switching Configuration Guide).

NOTE:
When MFF works with static IP source guard entries, you must configure VLAN IDs in the static entries. Otherwise, IP packets allowed by IP source guard are permitted even if their destination MAC addresses are not the MAC address of the gateway.
Basic concepts

An MFF-enabled device has two types of ports: user port and network port.

User port

An MFF user port is directly connected to a host and processes the following packets differently:

- Allows multicast packets to pass.
- Delivers ARP packets to the CPU.
- After learning gateways' MAC addresses, a user port allows only the unicast packets with the gateways' MAC addresses as the destination MAC addresses to pass. If no gateways' MAC addresses are learned, a user port discards all received unicast packets.

Network port

An MFF network port is connected to any of the following networking devices:

- An access switch.
- A distribution switch.
- A gateway.
- A server.

A network port processes the following packets differently:

- Allows multicast packets to pass.
- Delivers ARP packets to the CPU.
- Denies broadcast packets other than DHCP and ARP packets.

You need to configure the following ports as network ports:

- Upstream ports connected to a gateway.
- Ports connected to the MFF devices in a cascaded network (a network with multiple MFF devices connected to one another).
- Ports between devices in a ring network.

Link aggregation is supported by network ports in an MFF-enabled VLAN, but it is not supported by user ports in the VLAN. You can add the network ports to link aggregation groups, but cannot add the user ports to link aggregation groups. For more information about link aggregation, see Layer 2—LAN Switching Configuration Guide.

NOTE:

- A network port is not always an upstream port.
- If you enable MFF for a VLAN, each port in the VLAN must be a network or user port.

MFF operation modes

Manual mode

The manual mode applies to networks where the hosts' IP addresses are manually configured. The hosts cannot obtain the gateway information through DHCP. A VLAN maintains only the MAC address of the default gateway.

After receiving an ARP request for a host's MAC address from the gateway, the MFF device directly replies the host's MAC address to the gateway according to the ARP snooping entries. After learning the gateway's MAC address, the MFF device updates the MAC address upon receiving an ARP packet with a different sender MAC address from the default gateway.
MFF working mechanism

An MFF-enabled device implements Layer 3 communication between hosts by intercepting ARP requests from the hosts and replies with the MAC address of a gateway. This mechanism helps reduce the number of broadcast messages.

The MFF device processes ARP packets as follows:

- After receiving an ARP request from a host, the MFF device sends the MAC address of the corresponding gateway to the host. In this way, hosts in the network have to communicate at Layer 3 through a gateway.
- After receiving an ARP request from a gateway, the MFF device sends the requested host's MAC address to the gateway if the corresponding entry is available. If the entry is not available, the MFF device forwards the ARP request.
- The MFF device forwards ARP replies between hosts and gateways.
- If the source MAC addresses of ARP requests from gateways are different from those recorded, the MFF device updates and broadcasts the IP and MAC addresses of the gateways.

Protocols and standards

RFC 4562, MAC-Forced Forwarding

Configuring MFF

Enabling MFF

In MFF manual mode, enable ARP snooping on the device.

To enable MFF:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable MFF.</td>
<td>mac-forced-forwarding default-gateway gateway-ip</td>
</tr>
</tbody>
</table>

Configuring a network port

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.</td>
<td>• Layer 2 Ethernet interface view: interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Layer 2 aggregate interface view: interface bridge-aggregation interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the port as a network port.</td>
<td>mac-forced-forwarding network-port</td>
</tr>
</tbody>
</table>
Enabling periodic gateway probe

You can configure the MFF device to detect gateways every 30 seconds for the change of MAC addresses by sending forged ARP packets. The ARP packets use 0.0.0.0 as the sender IP address and bridge MAC address as the sender MAC address.

This feature is supported by MFF manual mode.

To enable periodic gateway probe:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>3.</td>
<td>Enable periodic gateway probe.</td>
<td>mac-forced-forwarding gateway probe</td>
</tr>
</tbody>
</table>

Specifying the IP addresses of servers

You must specify the servers on the MFF device to ensure communication between the servers and clients.

When the MFF device receives an ARP request from a server, the MFF device searches IP-to-MAC address entries it has stored. Then the device replies with the requested MAC address to the server. As a result, packets from a host to a server are forwarded by the gateway. However, packets from a server to a host are not forwarded by the gateway.

MFF does not check whether the IP address of a server is on the same network segment as that of a gateway. Instead, it checks whether the IP address of a server is all-zero or all-one. An all-zero or all-one server IP address is invalid.

You can specify a server's IP address in manual MFF mode.

To specify the IP addresses of servers:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VLAN view.</td>
<td>vlan vlan-id</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the IP addresses of servers.</td>
<td>mac-forced-forwarding server server-ip&amp;&lt;1-10&gt;</td>
</tr>
</tbody>
</table>

Displaying and maintaining MFF

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display MFF port configuration information.</td>
<td>display mac-forced-forwarding interface</td>
</tr>
</tbody>
</table>
MFF configuration examples

Manual-mode MFF configuration example in a tree network

Network requirements

As shown in Figure 131, all the devices are in VLAN 100. Hosts A, B, and C are assigned IP addresses manually.

Configure MFF to isolate the hosts at Layer 2 and allow them to communicate with each other through Gateway at Layer 3.

Figure 131 Network diagram

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the MFF configuration information for a VLAN.</td>
<td>display mac-forced-forwarding vlan vlan-id</td>
</tr>
</tbody>
</table>

Configuration procedure

1. Configure the IP addresses of the hosts and Gateway as shown in Figure 131.
2. Configure Switch A:

   # Configure manual-mode MFF on VLAN 100.
   [SwitchA] vlan 100
   [SwitchA-vlan100] mac-forced-forwarding default-gateway 10.1.1.100

   # Specify the IP address of the server.
   [SwitchA-vlan100] mac-forced-forwarding server 10.1.1.200

   # Enable ARP snooping on VLAN 100.
   [SwitchA-vlan100] arp snooping enable
   [SwitchA-vlan100] quit

   # Configure GigabitEthernet 1/0/2 as a network port.
   [SwitchA] interface gigabitethernet 1/0/2
   [SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port

3. Configure Switch B:

   # Configure manual-mode MFF on VLAN 100.
   [SwitchB] vlan 100
   [SwitchB-vlan100] mac-forced-forwarding default-gateway 10.1.1.100

   # Specify the IP address of the server.
**Manual-mode MFF configuration example in a ring network**

**Network requirements**

As shown in [Figure 132](#), all the devices are in VLAN 100, and the switches form a ring. Hosts A, B, and C are assigned IP addresses manually.

Configure MFF to isolate the hosts at Layer 2 and allow them to communicate with each other through Gateway at Layer 3.

**Figure 132 Network diagram**

![Network diagram](#)

**Configuration procedure**

1. Configure the IP addresses of the hosts and Gateway as shown in [Figure 132](#).
2. Configure Switch A:
   - # Enable STP globally to make sure STP is enabled on interfaces.
     ```
     [SwitchA] stp global enable
     ```
   - # Configure manual-mode MFF on VLAN 100.
     ```
     [SwitchA] vlan 100
     [SwitchA-vlan100] mac-forced-forwarding default-gateway 10.1.1.100
     ```
   - # Specify the IP address of the server.
     ```
     [SwitchA-vlan100] mac-forced-forwarding server 10.1.1.200
     ```
   - # Enable ARP snooping on VLAN 100.
     ```
     [SwitchA-vlan100] arp snooping enable
     [SwitchA-vlan100] quit
     ```
   - # Configure GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 as network ports.
     ```
     [SwitchA] interface gigabitethernet 1/0/2
     [SwitchA-GigabitEthernet1/0/2] mac-forced-forwarding network-port
     [SwitchA-GigabitEthernet1/0/2] quit
     ```
3. **Configure Switch B:**

   # Enable STP globally to make sure STP is enabled on interfaces.
   [SwitchB] stp global enable

   # Configure manual-mode MFF on VLAN 100.
   [SwitchB] vlan 100
   [SwitchB-vlan100] mac-forced-forwarding default-gateway 10.1.1.100

   # Specify the IP address of the server.
   [SwitchB-vlan100] mac-forced-forwarding server 10.1.1.200

   # Enable ARP snooping on VLAN 100.
   [SwitchB-vlan100] arp snooping enable
   [SwitchB-vlan100] quit

   # Configure GigabitEthernet 1/0/4 and GigabitEthernet 1/0/6 as network ports.
   [SwitchB] interface gigabitethernet 1/0/4
   [SwitchB-GigabitEthernet1/0/4] mac-forced-forwarding network-port
   [SwitchB-GigabitEthernet1/0/4] quit
   [SwitchB] interface gigabitethernet 1/0/6
   [SwitchB-GigabitEthernet1/0/6] mac-forced-forwarding network-port

4. **Enable STP on Switch C globally to make sure STP is enabled on interfaces.**

   <SwitchC> system-view
   [SwitchC] stp global enable
Configuring uRPF

Overview

Unicast Reverse Path Forwarding (uRPF) protects a network against source address spoofing attacks, such as DoS and DDoS attacks.

Attackers send packets with a forged source address to access a system that uses IP-based authentication, in the name of authorized users or even the administrator. Even if the attackers or other hosts cannot receive any response packets, the attacks are still disruptive to the attacked target.

Figure 133 Source address spoofing attack

As shown in Figure 133, an attacker on Router A sends the server (Router B) requests with a forged source IP address 2.2.2.1 at a high rate, and Router B sends response packets to IP address 2.2.2.1 (Router C). Consequently, both Router B and Router C are attacked. If the administrator disconnects Router C by mistake, the network service is interrupted.

Attackers can also send packets with different forged source addresses or attack multiple servers simultaneously to block connections or even break down the network.

uRPF can prevent these source address spoofing attacks. It checks whether an interface that receives a packet is the output interface of the FIB entry that matches the source address of the packet. If not, uRPF considers it a spoofing attack and discards the packet.

uRPF check modes

uRPF supports strict and loose modes.

- **Strict uRPF check**—To pass strict uRPF check, the source address of a packet and the receiving interface must match the destination address and output interface of a FIB entry. In some scenarios (for example, asymmetrical routing), strict uRPF might discard valid packets. Strict uRPF is often deployed between a PE and a CE.

- **Loose uRPF check**—To pass loose uRPF check, the source address of a packet must match the destination address of a FIB entry. Loose uRPF can avoid discarding valid packets, but might let go attack packets. Loose uRPF is often deployed between ISPs, especially in asymmetrical routing.

uRPF operation

Figure 134 shows how uRPF works.
1. uRPF checks source address validity:
   - uRPF discards packets with a broadcast source address.
   - uRPF discards packets with an all-zero source address but a non-broadcast destination address. (A packet with source address 0.0.0.0 and destination address 255.255.255.255 might be a DHCP or BOOTP packet and cannot be discarded.)
   - uRPF proceeds to step 2 for other packets.

2. uRPF checks whether the source address matches a FIB entry:
o If yes, uRPF proceeds to step 3.
o If no, uRPF proceeds to step 6.

3. uRPF checks whether the check mode is loose:
o If yes, uRPF proceeds to step 8.
o If no, uRPF checks whether the matching route is a direct route:
   – If yes, uRPF proceeds to step 5.
   – If no, uRPF proceeds to step 4.

4. uRPF checks whether the receiving interface matches the output interface of the matching FIB entry:
o If yes, uRPF proceeds to step 8.
o If no, uRPF proceeds to step 9.

5. uRPF checks whether the source IP address matches an ARP entry:
o If yes, uRPF proceeds to step 8.
o If no, uRPF proceeds to step 9.

6. uRPF checks whether the FIB table has a default route:
o If yes, uRPF proceeds to step 7.
o If no, uRPF proceeds to step 9.

7. uRPF checks whether the check mode is loose:
o If yes, uRPF proceeds to step 8.
o If no, uRPF checks whether the output interface of the default route matches the receiving interface of the packet:
   – If yes, uRPF proceeds to step 8.
   – If no, uRPF proceeds to step 9.

8. The packet passes the check and is forwarded.

9. The packet is discarded.

**NOTE:**
uRPF does not check multicast packets.
As shown in Figure 135, strict uRPF check is configured between an ISP network and a customer network. Loose uRPF check is configured between ISPs.

Enabling uRPF

When you enable uRPF, follow these restrictions and guidelines:

- Global uRPF configuration takes effect on both IPv4 and IPv6 routes.
- uRPF checks only incoming packets on an interface.
- After you enable the uRPF function on the switch, the routing table size might decrease by half.
- If the number of routes exceeds half the routing table size of the switch, the uRPF function cannot be enabled to avoid loss of routes and packets.

To enable uRPF globally:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>ip urpf { loose</td>
<td>strict }</td>
</tr>
</tbody>
</table>

Displaying and maintaining uRPF

Execute display commands in any view.
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display uRPF config.</td>
<td><code>display ip urpf [ slot slot-number ]</code></td>
</tr>
</tbody>
</table>

**uRPF configuration example**

**Network requirements**
As shown in Figure 136, a client (Switch A) directly connects to an ISP switch (Switch B). Enable strict uRPF check on Switch A and Switch B to prevent source address spoofing attacks.

**Figure 136 Network diagram**

**Configuration procedure**

1. Enable strict uRPF check on Switch A.
   
   `<SwitchA> system-view`  
   `
   [SwitchA] ip urpf strict`

2. Enable strict uRPF check on Switch B.
   
   `<SwitchB> system-view`  
   `
   [SwitchB] ip urpf strict`
Configuring crypto engines

Overview

Crypto engines encrypt and decrypt data for service modules. Crypto engines include the following types:

- **Hardware crypto engines**—A hardware crypto engine is a coprocessor integrated on a CPU or hardware crypto card. Hardware crypto engines can accelerate encryption/decryption speed, which improves device processing efficiency. You can enable or disable hardware crypto engines globally as needed.

- **Software crypto engines**—A software crypto engine is a set of software encryption algorithms. The device uses software crypto engines to encrypt and decrypt data for service modules. They are always enabled. You cannot enable or disable software crypto engines. The switch only supports software crypto engines in the current software version.

Crypto engines provide encryption/decryption services for service modules, for example, the IPsec module. When a service module requires data encryption/decryption, it sends the desired data to a crypto engine. After the crypto engine completes data encryption/decryption, it sends the data back to the service module.

Displaying and maintaining crypto engines

Execute **display** commands in any view and **reset** commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about crypto engines.</td>
<td><code>display crypto-engine</code></td>
</tr>
<tr>
<td>Display statistics for crypto engines.</td>
<td><code>display crypto-engine statistics [ engine-id engine-id slot slot-number ]</code></td>
</tr>
<tr>
<td>Clear statistics for crypto engines.</td>
<td><code>reset crypto-engine statistics [ engine-id engine-id slot slot-number ]</code></td>
</tr>
</tbody>
</table>
Configuring FIPS

Overview

Federal Information Processing Standards (FIPS) was developed by the National Institute of Standard and Technology (NIST) of the United States. FIPS specifies the requirements for cryptographic modules. FIPS 140-2 defines four levels of security, named Level 1 to Level 4, from low to high. The device supports Level 2.

Unless otherwise noted, in this document the term FIPS refers to FIPS 140-2.

Configuration restrictions and guidelines

When you configure FIPS, follow these restrictions and guidelines:

- After the `fips mode enable` command is executed, the system prompts you to choose a reboot method. If you do not make a choice within 30 seconds, the system uses the manual reboot method.
- Before you reboot the device to enter FIPS mode, the system automatically removes all key pairs configured in non-FIPS mode and all FIPS-incompliant digital certificates. FIPS-incompliant digital certificates are MD5-based certificates with the modulus length of key pairs less than 2048 bits. You cannot log in to the device through SSH after the device enters FIPS mode. To log in to the device in FIPS mode through SSH, first log in to the device through a console port, and then create a key pair for the SSH server.
- The password for entering the device in FIPS mode must comply with the password control policies, such as password length, complexity, and aging policy. When the aging timer for a password expires, the system prompts you to change the password. If you adjust the system time after the device enters FIPS mode, the login password might expire before the next login, because the original system time is typically much earlier than the actual time.
  - If you choose the automatic reboot method, set the system time before executing the `fips mode enable` command.
  - If you choose the manual reboot method, set the system time before configuring the local username and password.
- To use the manual reboot method to enter FIPS mode, you must perform the following tasks:
  a. Save the current configuration file.
  b. Specify the current configuration file as the startup configuration file.
  c. Delete the startup configuration file in binary format.
  d. Reboot the device.
Otherwise, the commands that are not supported by FIPS mode, if they are in the configuration file, might be restored.
- The system enters an intermediate state between when the `fips mode enable` command is executed and when the system is rebooted. If you choose the manual reboot method, do not execute any commands except for the following commands:
  - Reboot.
  - save.
  - Other commands used for configuration preparation to enter FIPS mode.
- Configuration rollback is supported in FIPS mode and also during a switch between FIPS mode and non-FIPS mode. After a configuration rollback between FIPS mode and non-FIPS mode, perform the following tasks:
Configuring FIPS mode

Entering FIPS mode

After you enable FIPS mode and reboot the device, the device operates in FIPS mode. The FIPS device has strict security requirements, and performs self-tests on cryptography modules to verify that they are operating correctly.

A FIPS device meets the requirements defined in Network Device Protection Profile (NDPP) of Common Criteria (CC).

The system provides two methods to enter FIPS mode: automatic reboot and manual reboot.

Automatic reboot

To use automatic reboot to enter FIPS mode:
1. Enable FIPS mode.
2. Select the automatic reboot method.
   The system automatically performs the following tasks:
   a. Create a default FIPS configuration file named fips-startup.cfg.
   b. Specify the default file as the startup configuration file.
   c. Prompt you to configure the username and password for next login.
   You can press Ctrl+C to exit the configuring process. Then, the fips mode enable command will not be executed.
3. Configure a username and password to log in to the device in FIPS mode.
   The password must include at least 15 characters that contain uppercase and lowercase letters, digits, and special characters.
   The system automatically uses the startup configuration file to reboot the device and enter FIPS mode. You can only use the configured username and password to log in to the FIPS device. After login, you are assigned the role of security administrator Crypto Officer.

Manual reboot

To use manual reboot to enter FIPS mode:
1. Enable the password control function globally.
2. Set the number of character types a password must contain to 4, and set the minimum number of characters for each type to one character.
3. Set the minimum length of user passwords to 15 characters.
4. Add a local user account for device management, including the following items:
   o A username.
o A password that complies with the password control policies in step 2 and step 3.
o A user role of network-admin.
o A service type of terminal.

5. Delete the FIPS-incompliant local user service types Telnet, HTTP, and FTP.
6. Enable FIPS mode.
7. Select the manual reboot method.
8. Save the configuration file and specify it as the startup configuration file.
9. Delete the startup configuration file in binary format (an .mdb file).
10. Reboot the device.

The system enters FIPS mode. You can use the configured username and password to log in to the device in FIPS mode.

To enable FIPS mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable FIPS mode.</td>
<td>fips mode enable</td>
</tr>
</tbody>
</table>

**Configuration changes in FIPS mode**

When the system enters FIPS mode, the following changes occur:

- The user login authentication mode can only be **scheme**.
- The FTP/TFTP server and client are disabled.
- The Telnet server and client are disabled.
- The HTTP server is disabled.
- SNMPv1 and SNMPv2c are disabled. Only SNMPv3 is available.
- The SSL server only supports TLS1.0, TLS1.1 and TLS1.2.
- The SSH server does not support SSHv1 clients and DSA key pairs.
- The generated RSA and DSA key pairs must have a modulus length of 2048 bits. When the device acts as a server to authenticate a client through the public key, the key pair for the client must also have a modulus length of 2048 bits.
- The generated ECDSA key pairs must have a modulus length of more than 256 bits. When the device acts as a server to authenticate a client through the public key, the key pair for the client must also have a modulus length of more than 256 bits.
- SSH, SNMPv3, IPsec, and SSL do not support DES, 3DES, RC4, or MD5.
- The password control function cannot be disabled globally. The **undo password-control enable** command does not take effect.
- The keys must contain at least 15 characters and 4 character types of uppercase and lowercase letters, digits, and special characters. This requirement applies to the following passwords:
  o AAA server's shared key.
  o IKE pre-shared key.
  o SNMPv3 authentication key.

The password for a device management local user and password for switching user roles depend on password control policies. By default, the passwords must contain at least 15
Exiting FIPS mode

After you disable FIPS mode and reboot the device, the device operates in non-FIPS mode.

The system provides two methods to exit FIPS mode: automatic reboot and manual reboot.

**Automatic reboot**

Select the automatic reboot method. The system automatically creates a default non-FIPS configuration file named `non-fips-startup.cfg`, and specifies the file as the startup configuration file. The system reboots the device by using the default non-FIPS configuration file. After the reboot, you are directly logged into the device.

**Manual reboot**

This method requires that you manually complete the configurations for entering non-FIPS mode, and then reboot the device. To log in to the device after the reboot, you must enter user information according to the authentication mode. The following default authentication modes are available for different ports or lines (you can modify the default mode as needed):

- The default authentication mode is `password` for VTY lines.
- The default authentication mode is `none` for a console port.

After you disable FIPS mode, follow these restrictions and guidelines before you manually reboot the device:

- If you are logged into the device through Telnet, perform the following tasks without exiting the current user line:
  - Set the authentication mode to `scheme`.
  - Configure the username and password. (You can also use the current username and password.)
- If you are logged into the device through a console port, configure one of the following authentication modes as needed:
  - Configure the `password` authentication mode and a password.
  - Configure the `scheme` authentication mode and configure a new username and password (you can also use the current username and password).
  - Configure the `none` authentication mode.

To disable FIPS mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Disable FIPS mode.</td>
<td><code>undo fips mode enable</code></td>
<td>By default, the FIPS mode is disabled.</td>
</tr>
</tbody>
</table>

**FIPS self-tests**

To ensure the correct operation of cryptography modules, FIPS provides self-test mechanisms, including power-up self-test and conditional self-test. You can also trigger a self-test. If the power-up self-test fails, the device where the self-test process exists reboots. If the conditional self-test fails, the system outputs self-test failure information.
NOTE: If a self-test fails, contact Hewlett Packard Enterprise Support.

Power-up self-tests

The power-up self-test examines the availability of FIPS-allowed cryptographic algorithms. The device supports the following types of power-up self-tests:

- **Known-answer test (KAT)**
  A cryptographic algorithm is run on data for which the correct output is already known. The calculated output is compared with the known answer. If they are not identical, the KAT test fails.

- **Pairwise conditional test (PWCT)**
  - Signature and authentication test—The test is run when a DSA, RSA, or ECDSA asymmetrical key pair is generated. It uses the private key to sign the specific data, and then uses the public key to authenticate the signed data. If the authentication is successful, the test succeeds.
  - Encryption and decryption test—The test is run when an RSA asymmetrical key pair is generated. It uses the public key to encrypt a plain text string, and then uses the private key to decrypt the encrypted text. If the decryption result is the same as the original plain text string, the test succeeds.

The power-up self-test examines the cryptographic algorithms listed in Table 21.

**Table 21 Power-up self-test list**

<table>
<thead>
<tr>
<th>Type</th>
<th>Operations</th>
</tr>
</thead>
</table>
| KAT  | Tests the following algorithms:  
  - 3DES.  
  - SHA1, SHA224, SHA256, SHA384, and SHA512.  
  - HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512.  
  - AES.  
  - RSA.  
  - ECDH.  
  - RNG.  
  - DRBG.  
  - GCM.  
  - GMAC.  |
| PWCT | Tests the following algorithms:  
  - RSA (signature and authentication).  
  - RSA (encryption and decryption).  
  - DSA (signature and authentication).  
  - ECDSA (signature and authentication).  |

Conditional self-tests

A conditional self-test runs when an asymmetrical cryptographic module or a random number generator module is invoked. Conditional self-tests include the following types:
• **Signature and authentication PWCT test**—This test is run when a DSA/RSA asymmetrical key pair is generated. It uses the private key to sign the specific data, and then uses the public key to authenticate the signed data. If the authentication is successful, the test succeeds.

• **Continuous random number generator test**—This test is run when a random number is generated. If two consecutive random numbers are different, the test succeeds. Otherwise, the test fails. This test can also be run when a DSA/RSA asymmetrical key-pair is generated.

**Triggering self-tests**

To examine whether the cryptography modules operate correctly, you can trigger a self-test on the cryptographic algorithms. The triggered self-test is the same as the power-up self-test. If the self-test fails, the device where the self-test process exists reboots.

To trigger a self-test:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2. Trigger a self-test.</td>
<td><code>fips self-test</code></td>
</tr>
</tbody>
</table>

**Displaying and maintaining FIPS**

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the FIPS mode state.</td>
<td><code>display fips status</code></td>
</tr>
</tbody>
</table>

**FIPS configuration examples**

**Entering FIPS mode through automatic reboot**

**Network requirements**

Use the automatic reboot method to enter FIPS mode, and use a console port to log in to the device in FIPS mode.

**Configuration procedure**

# If you want to save the current configuration, execute the `save` command before you enable FIPS mode.

# Enable FIPS mode and choose the automatic reboot method to enter FIPS mode. Set the username to `root` and the password to `12345zxcvbl@#$%ZXCVB`.

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:y
The system will create a new startup configuration file for FIPS mode. After you set the login username and password for FIPS mode, the device will reboot automatically.
Enter username(1-55 characters):root
Enter password(15-63 characters):
```
Confirm password:  
Waiting for reboot... After reboot, the device will enter FIPS mode.

Verifying the configuration

After the device reboots, enter a username of root and a password of 12345zxcvb1@#$%ZXCVB. The system prompts you to configure a new password. After you configure the new password, the device enters FIPS mode. The new password must be different from the previous password. It must include at least 15 characters, and contain uppercase and lowercase letters, digits, and special characters. For more information about the requirements for the password, see the system output.

Press ENTER to get started.

login: root
Password:
First login or password reset. For security reason, you need to change your password. Please enter your password.
old password:
new password:
confirm:
Updating user information. Please wait ... ... ...
...
<Sysname>

# Display the current FIPS mode state.
<Sysname> display fips status
FIPS mode is enabled.

# Display the default configuration file.
<Sysname> more fips-startup.cfg
#
password-control enable
#
local-user root class manage
  service-type terminal
  authorization-attribute user-role network-admin
#
fips mode enable
#
return

<Sysname>

Entering FIPS mode through manual reboot

Network requirements

Use the manual reboot method to enter FIPS mode, and use a console port to log in to the device in FIPS mode.

Configuration procedure

# Enable the password control function globally.
<Sysname> system-view
[Sysname] password-control enable
# Set the number of character types a password must contain to 4, and set the minimum number of characters for each type to one character.

```
[Sysname] password-control composition type-number 4 type-length 1
```

# Set the minimum length of user passwords to 15 characters.

```
[Sysname] password-control length 15
```

# Add a local user account for device management, including a username of test, a password of 12345zxcvbl@#$%ZXCVB, a user role of network-admin, and a service type of terminal.

```
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password simple 12345zxcvbl@#$%ZXCVB
[Sysname-luser-manage-test] authorization-attribute user-role network-admin
[Sysname-luser-manage-test] service-type terminal
[Sysname-luser-manage-test] quit
```

# Enable FIPS mode, and choose the manual reboot method to enter FIPS mode.

```
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:n
Change the configuration to meet FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter FIPS mode.
```

# Save the current configuration to the root directory of the storage medium, and specify it as the startup configuration file.

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to device successfully.
[Sysname] quit
```

# Delete the startup configuration file in binary format.

```
<Sysname> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.
```

# Reboot the device.

```
<Sysname> reboot
```

### Verifying the configuration

After the device reboots, enter a username of test and a password of 12345zxcvbl@#$%ZXCVB. The system prompts you to configure a new password. After you configure the new password, the device enters FIPS mode. The new password must be different from the previous password. It must include at least 15 characters, and contain uppercase and lowercase letters, digits, and special characters. For more information about the requirements for the password, see the system output.

Press ENTER to get started.

```
login: test
Password:
First login or password reset. For security reason, you need to change your pass
word. Please enter your password.
old password:
n new password:
confirm:
```
Exiting FIPS mode through automatic reboot

Network requirements
A user has logged in to the device in FIPS mode through a console port.
Use the automatic reboot method to exit FIPS mode.

Configuration procedure

# Disable FIPS mode.
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode and then reboot automatically. Continue? [Y/N]:y
Waiting for reboot... After reboot, the device will enter non-FIPS mode.

Verifying the configuration
After the device reboots, you can enter the system.

# Display the current FIPS mode state.
<Sysname> display fips status
FIPS mode is disabled.

Exiting FIPS mode through manual reboot

Network requirements
A user has logged in to the device in FIPS mode through SSH with a username of test and a password of 12345zxcvbl@#$%^ZXCVB.
Use the manual reboot method to exit FIPS mode.

Configuration procedure

# Disable FIPS mode.
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode, and then reboot automatically. Continue? [Y/N]:n
Change the configuration to meet non-FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter non-FIPS mode.

# Set the authentication mode for VTY lines to scheme.
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme

# Save the current configuration to the root directory of the storage medium, and specify it as the startup configuration file.
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to device successfully.
[Sysname] quit

# Delete the startup configuration file in binary format.
<Sysname> delete flash:/startup.mdb
Delete flash:/startup.mdb?[Y/N]:y
Deleting file flash:/startup.mdb...Done.

# Reboot the device.
<Sysname> reboot

Verifying the configuration

After the device reboots, enter a username of test and a password of 12345zxcvb!@#$%ZXCVB to enter non-FIPS mode.
Press ENTER to get started.
login: test
Password:
Last successfully login time:...
...
<Sysname>

# Display the current FIPS mode state.
<Sysname> display fips status
FIPS mode is disabled.
Configuring user profiles

Overview

A user profile saves a set of predefined parameters, such as a QoS policy.

The user profile application allows flexible traffic policing on a per-user basis. Each time a user passes authentication, the device automatically applies the parameters in the user profile to this user.

The user profile restricts authenticated user behaviors as follows:
1. After the authentication server verifies a user, the server sends the device the name of the user profile specified for the user.
2. The device applies the parameters in the user profile to the user.
3. When the user logs out, the device automatically removes the user profile parameters.

Configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Creating a user profile</td>
</tr>
<tr>
<td>(Required.) Configuring QoS parameters for traffic management</td>
</tr>
</tbody>
</table>

Configuration restrictions and guidelines

Before creating a user profile, perform the following tasks:
1. Plan the authentication method for your network. The user profile supports working with 802.1X and MAC authentication.
   - In remote authentication, specify a user profile for each user account on the authentication server.
   - In local authentication, specify a user profile for each user account in the local user view. For more information, see "Configuring AAA."
2. Configure the authentication parameters on the client, the device, and the authentication server. The parameters include username, password, authentication scheme, and authentication domain.

Creating a user profile

To create a user profile:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a user profile and enter user profile view.</td>
<td>user-profile profile-name</td>
</tr>
</tbody>
</table>
Configuring parameters for a user profile

Configurations in user profile view take effect only after the device applies the user profile to the user.

Configuring QoS parameters for traffic management

To configure QoS parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>user-profile profile-name</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>qos apply policy</td>
<td>The QoS policy must already exist. For information about QoS policy</td>
</tr>
<tr>
<td></td>
<td>policy-name</td>
<td>configuration, see ACL and QoS Configuration Guide.</td>
</tr>
<tr>
<td></td>
<td>{ inbound</td>
<td>outbound }</td>
</tr>
</tbody>
</table>

Displaying and maintaining user profiles

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display configuration and online user information for the specified user profile or all user profiles.</td>
<td><code>display user-profile [ name profile-name ] [ slot slot-number ]</code></td>
</tr>
</tbody>
</table>

User profile configuration examples

Local 802.1X authentication/authorization with QoS policy configuration example

Network requirements

As shown in Figure 137, the access switch performs local 802.1X authentication and authorization for User A, User B, and User C.

Configure user profiles for the users and apply a QoS policy to each user to implement the following functions:

- Deny User A’s access to the network from 8:30 to 12:00 daily.
- Limit the outgoing traffic rate to 2000 kbps for User B.
- Limit the incoming traffic rate to 4000 kbps for User C.
Configuration procedure

1. Configure a QoS policy to control the access time for User A:
   # Create periodic time range for_usera, setting it to be active from 8:30 to 12:00 daily.
   [Switch] time-range for_usera 8:30 to 12:00 daily
   # Configure IPv4 basic ACL 2000 to identify packets in time range for_usera.
   [Switch] acl number 2000
   [Switch-acl-basic-2000] rule permit time-range for_usera
   [Switch-acl-basic-2000] quit
   # Create traffic class for_usera, and define a match criterion to match ACL 2000.
   [Switch] traffic classifier for_usera
   [Switch-classifier-for_usera] if-match acl 2000
   [Switch-classifier-for_usera] quit
   # Create traffic behavior for_usera, and configure a traffic filtering action as deny.
   [Switch] traffic behavior for_usera
   [Switch-behavior-for_usera] filter deny
   [Switch-behavior-for_usera] quit
   # Create QoS policy for_usera, and associate traffic class for_usera with traffic behavior for_usera.
   [Switch] qos policy for_usera
   [Switch-qospolicy-for_usera] classifier for_usera behavior for_usera
   [Switch-qospolicy-for_usera] quit

2. Configure a user profile for User A, and apply the QoS policy:
   # Create user profile usera.
   [Switch] user-profile usera
   # Apply the QoS policy to the incoming traffic of the switch.
   [Switch-user-profile-usera] qos apply policy for_usera inbound
   [Switch-user-profile-usera] quit

3. Configure a QoS policy to limit the outgoing traffic rate of User B:
   # Create traffic class class, and define a match criterion to match all packets.
   [Switch] traffic classifier class
   [Switch-classifier-class] if-match any
   [Switch-classifier-class] quit
# Create traffic behavior for_userb, and configure a CAR action in traffic behavior database.
Set the CIR to 2000 kbps.

```bash
[Switch] traffic behavior for_userb
[Switch-behavior-for_userb] car cir 2000
[Switch-behavior-for_userb] quit
```

# Create QoS policy for_userb, and associate traffic class class with traffic behavior for_userb.

```bash
[Switch] qos policy for_userb
[Switch-qospolicy-for_userb] classifier class behavior for_userb
[Switch-qospolicy-for_userb] quit
```

4. Configure a user profile for User B, and apply the QoS policy:

# Create user profile userb.

```bash
[Switch] user-profile userb
```

# Apply the QoS policy to the incoming traffic of the switch.

```bash
[Switch-user-profile-userb] qos apply policy for_userb inbound
[Switch-user-profile-userb] quit
```

5. Configure a QoS policy to limit the incoming traffic rate on User C:

# Create traffic behavior for_userc, and configure a CAR action in traffic behavior database.
Set the CIR to 4000 kbps.

```bash
[Switch] traffic behavior for_userc
[Switch-behavior-for_userc] car cir 4000
[Switch-behavior-for_userc] quit
```

# Create QoS policy for_userc, and associate traffic class class with traffic behavior for_userc.

```bash
[Switch] qos policy for_userc
[Switch-qospolicy-for_userc] classifier class behavior for_userc
[Switch-qospolicy-for_userc] quit
```

6. Configure a user profile for User C, and apply the QoS policy:

# Create user profile userc.

```bash
[Switch] user-profile userc
```

# Apply the QoS policy to the outgoing traffic of the switch.

```bash
[Switch-user-profile-userc] qos apply policy for_userc outbound
[Switch-user-profile-userc] quit
```

7. Add local users:

# Add local user usera.

```bash
[Switch] local-user usera class network
New local user added.
```

# Set the password of local user usera to a12345 in plain text.

```bash
[Switch-luser-network-usera] password simple a12345
```

# Specify the service type as lan-access for usera.

```bash
[Switch-luser-network-usera] service-type lan-access
```

# Configure the authorization user profile as usera.

```bash
[Switch-luser-network-usera] authorization-attribute user-profile usera
[Switch-luser-network-usera] quit
```

# Add local user userb.

```bash
[Switch] local-user userb class network
New local user added.
```
# Set the password of local user userb to b12345 in plain text.
[Switch-luser-network-userb] password simple b12345

# Specify the service type as lan-access for userb.
[Switch-luser-network-userb] service-type lan-access

# Configure the authorization user profile as userb.
[Switch-luser-network-userb] authorization-attribute user-profile userb
[Switch-luser-network-userb] quit

# Add local user userc.
[Switch] local-user userc class network
New local user added.

# Set the password of local user userc to c12345 in plain text.
[Switch-luser-network-userc] password simple c12345

# Specify the service type as lan-access for userc.
[Switch-luser-network-userc] service-type lan-access

# Configure the authorization user profile as userc.
[Switch-luser-network-userc] authorization-attribute user-profile userc
[Switch-luser-network-userc] quit

8. Configure the authentication, authorization, and accounting method for local users:

# Configure ISP domain user to use local authentication and authorization without accounting for local users.
[Switch] domain user
[Switch-isp-user] authentication lan-access local
[Switch-isp-user] authorization lan-access local
[Switch-isp-user] accounting login none
[Switch-isp-user] quit

9. Configure 802.1X:

# Enable 802.1X on GigabitEthernet 1/0/1.
[Switch] interface gigabitethernet 1/0/1
[Switch-A-GigabitEthernet1/0/1] dot1x

# Configure Ten-GigabitEthernet 1/0/1 to implement MAC-based access control (the default).
[Switch-GigabitEthernet1/0/1] dot1x port-method macbased
[Switch-GigabitEthernet1/0/1] quit

# Enable 802.1X globally.
[Switch] dot1x

Verifying the configuration

# Use the correct usernames and passwords to access the network from User A, User B, and User C. A username must include the ISP domain name. For example, enter username usera@user and password a12345 for User A.

# Verify that the user profiles are active for User A, User B, and User C.

<Switch> display user-profile
User-Profile: usera
Inbound:
    Policy: for_usera

slot 1:
    User -:
        Authentication type: 802.1X

458
Network attributes:
  Interface : GigabitEthernet1/0/1
  MAC address : 6805-ca06-557b
  Service VLAN : 1

User-Profile: userb
Inbound:
  Policy: for_userb

slot 1:
  User -:
    Authentication type: 802.1X

Network attributes:
  Interface : GigabitEthernet1/0/1
  MAC address : 80c1-6ee0-2664
  Service VLAN : 1

User-Profile: userc
Outbound:
  Policy: for_userc

slot 1:
  User -:
    Authentication type: 802.1X

Network attributes:
  Interface : GigabitEthernet1/0/1
  MAC address : 6805-ca05-3efa
  Service VLAN : 1
Configuring attack detection and prevention

Overview

Attack detection and prevention enables a device to detect attacks by inspecting arriving packets, and to take prevention actions, such as packet dropping, to protect a private network.

The device supports only TCP fragment attack prevention.

Configuring TCP fragment attack prevention

The TCP fragment attack prevention feature enables the device to drop attack TCP fragments to prevent TCP fragment attacks that traditional packet filter cannot detect. As defined in RFC 1858, attack TCP fragments refer to the following TCP fragments:

- First fragments in which the TCP header is smaller than 20 bytes.
- Non-first fragments with a fragment offset of 8 bytes (FO=1).

To configure TCP fragment attack prevention:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enable TCP fragment attack prevention.</td>
<td><strong>attack-defense tcp fragment enable</strong></td>
</tr>
</tbody>
</table>
Configuring MACsec

Overview

Media Access Control Security (MACsec) secures data communication on IEEE 802 LANs. MACsec provides services such as data encryption, frame integrity check, and data origin validation for frames on the MAC sublayer of the Data Link Layer.

Basic concepts

CA

Connectivity association (CA) is a group of participants that use the same key and key algorithm. The encryption key used by the CA participants is called a connectivity association key (CAK). The following types of CAKs are available:

- **Pairwise CAK**—Used by CAs that have two participants.
- **Group CAK**—Used by CAs that have more than two participants.

The pairwise CAK is used most often because MACsec is typically applied to point-to-point networks.

A CAK can be an encryption key generated during 802.1X authentication or a user-configured preshared key. The user-configured preshared key takes precedence over the 802.1X-generated key.

SA

Secure association (SA) is an agreement negotiated by CA participants. The agreement includes a cipher suite and keys for integrity check.

A secure channel can contain more than one SA. Each SA uses a unique secure association key (SAK). The SAK is generated from the CAK, and MACsec uses the SAK to encrypt data transmitted along the secure channel.

MACsec Key Agreement (MKA) limits the number of packets that can be encrypted by an SAK. When the limit is exceeded, the SAK will be refreshed. For example, when packets with the minimum size are sent on a 10-Gbps link, an SAK rekey occurs about every 300 seconds.

MACsec services

MACsec provides the following services:

- **Data encryption**—Enables a port to encrypt outbound frames and decrypt MACsec-encrypted inbound frames.

- **Integrity check**—Performs integrity check when the device receives a MACsec-encrypted frame. The integrity check uses the following process:
  a. Uses a key negotiated by MKA to calculate an integrity check value (ICV) for the frame.
  b. Compares the calculated ICV with the ICV in the frame trailer.
     - If the ICVs are the same, the device verifies the frame as legal.
     - If the ICVs are different, the device determines whether to drop the frame based on the validation mode.

- **MACsec replay protection**—When MACsec frames are transmitted over the network, frame disorder might occur. MACsec replay protection allows the device to accept the out-of-order packets within the replay protection window size and drop other out-of-order packets.
MACsec applications

MACsec supports the following application modes:

- **Client-oriented mode**—Secures data transmission between the client and the access device. In this mode, the authentication server generates and distributes the CAK-related parameters to the client and the access device. In this mode, MACsec must operate with 802.1X authentication.

  **Figure 138 Client-oriented mode**

  ![Client-oriented mode diagram](image)

  **NOTE:**

  In client-oriented mode, an MKA-enabled port on the access device must perform port-based 802.1X access control. The authentication method must be EAP relay.

- **Device-oriented mode**—Secures data transmission between devices. In this mode, the devices do not perform identity authentication, and the same preshared key must be configured on the MACsec ports that connect the devices. The devices use the configured preshared key as the CAK.

  **Figure 139 Device-oriented mode**

  ![Device-oriented mode diagram](image)

MACsec operating mechanism

**Operating mechanism for client-oriented mode**

**Figure 140** illustrates how MACsec operates in client-oriented mode.
The following shows the MACsec process:

1. After the client passes 802.1X authentication, the RADIUS server distributes the generated CAK-related parameters to the client and the access device.
2. After receiving the CAK, the client and the access device exchange EAPOL-MKA packets. The client and the access device exchange the MACsec capability and required parameters for session establishment. The parameters include MKA key server priority and MACsec desire. During the negotiation process, the access device automatically becomes the key server. The key server generates an SAK from the CAK for packet encryption, and it distributes the SAK to the client.
3. The client and the access device use the SAK to encrypt packets, and they send and receive the encrypted packets in secure channels.
4. When the access device receives a logoff request from the client, it immediately removes the associated secure session from the port. The remove operation prevents an unauthorized client from using the secure session established by the previous authorized client to access the network.

The MKA protocol also defines a session keepalive timer. If one participant does not receive any MKA packets from the peer after the timer expires, the participant removes the established secure session. The keepalive time is 6 seconds.
Operating mechanism for device-oriented mode

As shown in Figure 141, the devices use the configured preshared keys to start the session negotiation.

In this mode, the session negotiation, secure communication, and session termination processes are the same as the processes in client-oriented mode. However, MACsec performs a key server selection in this mode. The port with higher MKA key server priority becomes the key server, which is responsible for the generation and distribution of SAKs.

Figure 141 MACsec interactive process in device-oriented mode

Protocols and standards

- IEEE 802.1X-2010, Port-Based Network Access Control
- IEEE 802.1X-2006, Media Access Control (MAC) Security

Compatibility information

Feature and hardware compatibility

MKA cannot be enabled on MACsec-incapable interfaces. In this switch series, the following interfaces are MACsec-capable:

- The leftmost eight interfaces (GigabitEthernet x/0/1 through GigabitEthernet x/0/8) on each switch.
- The interfaces on HPE 5130/5510 10GBASE-T 2-port Module(JH156A), HPE 5130/5510 10GbE SFP+ 2-port Module(JH157A) interface modules installed on switch models except HPE 5510 24G SFP 4SFP+ HI 1-slot Switch(JH149A). The interface modules do not support hot swapping if MKA is enabled on such interfaces.

Feature and software version compatibility

The MACsec feature is available in Release 1121 and later.
MACsec configuration task list

In device-oriented mode, the MACsec configuration takes effect on Layer 2 and Layer 3 Ethernet ports. In client-oriented mode, the MACsec configuration takes effect only on 802.1X-enabled ports. To configure MACsec, perform the following tasks:

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(Required.) Enabling MKA</strong></td>
<td><strong>N/A</strong></td>
</tr>
<tr>
<td><strong>(Optional.) Enabling MACsec desire</strong></td>
<td><strong>N/A</strong></td>
</tr>
<tr>
<td><strong>(Optional.) Configuring a preshared key</strong></td>
<td><strong>This task is required in device-oriented mode.</strong></td>
</tr>
<tr>
<td><strong>(Optional.) Configuring the MKA key server priority</strong></td>
<td><strong>N/A</strong></td>
</tr>
<tr>
<td><strong>(Optional.) Use one of the following methods to configure MACsec protection parameters:</strong></td>
<td></td>
</tr>
<tr>
<td>• Configuring MACsec protection parameters in interface view:</td>
<td></td>
</tr>
<tr>
<td>o Configuring the MACsec confidentiality offset</td>
<td></td>
</tr>
<tr>
<td>o Configuring MACsec replay protection</td>
<td></td>
</tr>
<tr>
<td>o Configuring the MACsec validation mode</td>
<td></td>
</tr>
<tr>
<td>• Configuring MACsec protection parameters by MKA policy:</td>
<td></td>
</tr>
<tr>
<td>o Configuring an MKA policy</td>
<td></td>
</tr>
<tr>
<td>o Applying an MKA policy</td>
<td></td>
</tr>
</tbody>
</table>

Enabling MKA

MKA establishes and manages MACsec secure channels on a port. It also negotiates keys used by MACsec. You cannot enable MKA on a MACsec-incapable port.

To enable MKA:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>N/A</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>N/A</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Enable MKA.</td>
<td>mka enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, MKA is disabled on the port.</td>
</tr>
</tbody>
</table>

Enabling MACsec desire

The MACsec desire feature expects MACsec protection for outbound frames. The key server determines whether MACsec protects the outbound frames. MACsec protects the outbound frames of a port when the following requirements are met:

- The key server is MACsec capable.
- Both the local participant and its peer are MACsec capable.
A minimum of one participant is enabled with MACsec desire.

To enable MACsec desire:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface _interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Enable MACsec desire.</td>
<td>macsec desire</td>
</tr>
</tbody>
</table>

**Configuring a preshared key**

In device-oriented mode, configure a preshared key as the CAK to be used during MKA negotiation. To successfully establish an MKA session between two devices, make sure the connected MACsec ports are configured with the same preshared key.

A user-configured preshared key has higher priority than the 802.1X-generated CAK. To ensure a successful MKA session establishment, do not configure a preshared key in client-oriented mode.

To configure a preshared key:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter interface view.</td>
<td>interface _interface-type interface-number</td>
</tr>
</tbody>
</table>
| 3.   | Configure a preshared key. | mka psk ckn name cak simple value | By default, no MKA preshared key exists on the port. The MACsec cipher suite supported by HPE devices requires that the CKN and CAK each must be 32 characters long. If the configured CKN or CAK is not 32 characters long, the system performs the following operations when it runs the cipher suite:  
- Automatically increases the length of the CKN or CAK by zero padding if the CKN or CAK contains less than 32 characters.  
- Uses only the first 32 characters if the CKN or CAK contains more than 32 characters. |

**Configuring the MKA key server priority**

Configure an MKA key server priority for key server selection. The lower the priority value, the higher the priority.
In client-oriented mode, the access device port automatically becomes the key server. You do not have to configure the MKA key server priority.

In device-oriented mode, the port that has higher priority becomes the key server. If a port and its peers have the same priority, MACsec compares the secure channel identifier (SCI) values on the ports. The port with the lowest SCI value (a combination of MAC address and port ID) becomes the key server.

A port with priority 255 cannot become the key server. For a successful key server selection, make sure a minimum of one participant's key server priority is not 255.

To configure the MKA key server priority:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>mka priority priority-value</td>
<td>The default setting is 0.</td>
</tr>
</tbody>
</table>

Configuring MACsec protection parameters in interface view

If you configure a parameter in interface view after applying an MKA policy, the configuration in interface view overwrites the configuration of the parameter in the MKA policy. Your configuration also removes the MKA policy application from the port. However, other parameter settings of the MKA policy are effective on the port.

If the parameter value in interface view is the same as the value in the MKA policy, your configuration does not take effect. The policy remains active on the port.

Configuring the MACsec confidentiality offset

The MACsec confidentiality offset specifies the number of bytes starting from the frame header. MACsec encrypts only the bytes after the offset in a frame.

MACsec uses the confidentiality offset propagated by the key server.

To configure the MACsec confidentiality offset:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>macsec confidentiality-offset offset-value</td>
<td>The default setting is 0, and the entire frame needs to be encrypted. The offset value can be 0, 30, or 50.</td>
</tr>
</tbody>
</table>
Configuring MACsec replay protection

The MACsec replay protection feature allows a MACsec port to accept a number of out-of-order or repeated inbound frames. The configured replay protection window size is effective only when MACsec replay protection is enabled.

To configure MACsec replay protection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>macsec enable replay-protection</td>
<td>By default, MACsec replay protection is enabled on the port.</td>
</tr>
<tr>
<td>4.</td>
<td>macsec replay-protection window-size size-value</td>
<td>The default setting is 0, and frames are accepted only in the correct order.</td>
</tr>
</tbody>
</table>

Configuring the MACsec validation mode

The MACsec validation allows a port to perform integrity check based on the following validation modes:

- **check**—Performs validation only, and does not drop illegal frames.
- **disabled**—Does not perform validation.
- **strict**—Performs validation, and drops illegal frames.

In the current software version, only the **strict** mode is supported.

To configure the MACsec validation mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>macsec validation mode { check</td>
<td>disabled</td>
</tr>
</tbody>
</table>

Configuring MACsec protection parameters by MKA policy

Configuring an MKA policy

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>mka policy policy-name</td>
<td>By default, an MKA policy named <strong>default-policy</strong> exists.</td>
</tr>
</tbody>
</table>
### Applying an MKA policy

MKA policy provides a centralized method to configure MACsec confidentiality offset, replay protection, and validation mode. An MKA policy can be applied to a port or multiple ports. When you apply an MKA policy to a port, follow these restrictions and guidelines:

- The MACsec parameter settings configured in the MKA policy overwrite the MACsec parameters previously configured on the port.
- Any modifications to the MKA policy take effect immediately.
- When you remove an MKA policy application from the port, the MACsec parameter settings on the port restore to the default.
- When you apply a nonexistent MKA policy to the port, the port automatically uses the default MKA policy. If you create the policy, the policy will be automatically applied to the port.

To apply an MKA policy to a port:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>interface interface-type interface-number enable</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>mka apply policy policy-name</td>
<td>By default, no MKA policy is applied to the port.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining MACsec

Execute `display` commands in any view and `reset` commands in user view.
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display MACsec information on ports.</td>
<td><code>display macsec [ interface interface-type interface-number ] [ verbose ]</code></td>
</tr>
<tr>
<td>Display MKA session information.</td>
<td>`display mka session [ interface interface-type interface-number</td>
</tr>
<tr>
<td>Display MKA policy information.</td>
<td>`display mka { default-policy</td>
</tr>
<tr>
<td>Display MKA statistics on ports.</td>
<td><code>display mka statistics [ interface interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Reset MKA sessions on ports.</td>
<td><code>reset mka session [ interface interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Clear MKA statistics on ports.</td>
<td><code>reset mka statistics [ interface interface-type interface-number ]</code></td>
</tr>
</tbody>
</table>

**MACsec configuration examples**

**Client-oriented MACsec configuration example**

**Network requirements**

As shown in Figure 142, the host accesses the network through GigabitEthernet 1/0/1. The device performs RADIUS-based 802.1X authentication for the host to control user access to the Internet.

To ensure secure communication between the host and device, perform the following tasks on the device:

- Enable MACsec desire, and configure MKA to negotiate SAKs for packet encryption.
- Set the MACsec confidentiality offset to 30 bytes.
- Enable MACsec replay protection, and set the replay protection window size to 100.
- Set the MACsec validation mode to `strict`.

**Figure 142 Network diagram**

![Network diagram](image)

**Configuration procedure**

1. Configure the RADIUS server to provide authentication, authorization, and accounting services. Add a user account for the host. (Details not shown.)
2. Configure IP addresses for the Ethernet ports. (Details not shown.)
3. Configure AAA:
# Enter system view.
<Device> system-view

# Configure RADIUS scheme radius1.
[Device] radius scheme radius1
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
[Device-radius-radius1] key authentication simple name
[Device-radius-radius1] key accounting simple money
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit

# Configure authentication domain bbb for 802.1X users.
[Device] domain bbb
[Device-isp-bbb] authentication lan-access radius-scheme radius1
[Device-isp-bbb] authorization lan-access radius-scheme radius1
[Device-isp-bbb] accounting lan-access radius-scheme radius1
[Device-isp-bbb] quit

4. Configure 802.1X:
# Enable 802.1X on GigabitEthernet 1/0/1.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
# Implement port-based access control on GigabitEthernet 1/0/1.
[Device-GigabitEthernet1/0/1] dot1x port-method portbased
# Specify the mandatory authentication domain as bbb for 802.1X users on GigabitEthernet 1/0/1.
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
[Device-GigabitEthernet1/0/1] quit
# Enable 802.1X globally, and sets the device to relay EAP packets.
[Device] dot1x
[Device] dot1x authentication-method eap

5. Configure MACsec:
# Create an MKA policy named pls.
[Device] mka policy pls
# Set the MACsec confidentiality offset to 30 bytes.
[Device-mka-policy-pls] confidentiality-offset 30
# Enable MACsec replay protection.
[Device-mka-policy-pls] replay-protection enable
# Set the MACsec replay protection window size to 100.
[Device-mka-policy-pls] replay-protection window-size 100
# Set the MACsec validation mode to strict.
[Device-mka-policy-pls] validation mode strict
[Device-mka-policy-pls] quit
# Apply the MKA policy to GigabitEthernet 1/0/1.
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mka apply policy pls
# Configure MACsec desire and enable MKA on GigabitEthernet 1/0/1.
[Device-GigabitEthernet1/0/1] macsec desire
[Device-GigabitEthernet1/0/1] mka enable
Verifying the configuration

# Display MACsec information on GigabitEthernet 1/0/1.

[Device] display macsec interface gigabitethernet 1/0/1 verbose

Interface GigabitEthernet1/0/1
Protect frames : Yes
Active MKA policy : pls
Replay protection : Enabled
Replay window size : 100 frames
Confidentiality offset : 30 bytes
Validation mode : Strict
Included SCI : No
SCI conflict : No
Cipher suite : GCM-AES-128

Transmit secure channel:
SCI : 00E00100000A0006
Elapsed time: 00h:02m:07s
Current SA : AN 0 PN 1

Receive secure channels:
SCI : 00E0020000000106
Elapsed time: 00h:02m:03s
Current SA : AN 0 LPN 1
Previous SA : AN N/A LPN N/A

# Display MKA session information on GigabitEthernet 1/0/1 after a user logs in.

[Device] display mka session interface gigabitethernet 1/0/1 verbose

Interface GigabitEthernet1/0/1
Tx-SCI : 00E00100000A0006
Priority : 0
Capability: 3

CKN for participant: 1234
Key server : Yes
MI (MN) : A1E0D2897596817209CD2307 (2509)
Live peers : 1
Potential peers : 0
Principal actor : Yes
MKA session status : Secured
Confidentiality offset: 30 bytes
Current SAK status : Rx & Tx
Current SAK AN : 0
Current SAK KI (KN) : A1E0D2897596817209CD230700000002 (2)
Previous SAK status : N/A
Previous SAK AN : N/A
Previous SAK KI (KN) : N/A
Live peer list:

<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Priority</th>
<th>Capability</th>
<th>Rx-SCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2CAF896C9BFE2ABFB135E63</td>
<td>2512</td>
<td>0</td>
<td>3</td>
<td>00E0020000000106</td>
</tr>
</tbody>
</table>
Device-oriented MACsec configuration example

Network requirements

As shown in Figure 143, Device A is the MACsec key server.

To secure data transmission between the two devices by MACsec, perform the following tasks on Device A and Device B, respectively:

- Set the MACsec confidentiality offset to 30 bytes.
- Enable MACsec replay protection, and set the replay protection window size to 100.
- Set the MACsec validation mode to **strict**.
- Configure the CAK name (CKN) and the CAK as E9AC and 09DB3EF1, respectively.

Figure 143 Network diagram

![Network Diagram](image)

Configuration procedure

1. Configure Device A:

   # Enter system view.
   ```
   <DeviceA> system-view
   ```
   
   # Enter GigabitEthernet 1/0/1 interface view.
   ```
   [DeviceA] interface gigabitethernet 1/0/1
   ```
   
   # Enable MACsec desire on GigabitEthernet 1/0/1.
   ```
   [DeviceA-GigabitEthernet1/0/1] macsec desire
   ```
   
   # Set the MKA key server priority to 5.
   ```
   [DeviceA-GigabitEthernet1/0/1] mka priority 5
   ```
   
   #Configure the CKN as E9AC and the CAK as 09DB3EF1 in plain text.
   ```
   [DeviceA-GigabitEthernet1/0/1] mka psk ckn E9AC cak simple 09DB3EF1
   ```
   
   # Set the MACsec confidentiality offset to 30 bytes.
   ```
   [DeviceA-GigabitEthernet1/0/1] macsec confidentiality-offset 30
   ```
   
   # Enable MACsec replay protection.
   ```
   [DeviceA-GigabitEthernet1/0/1] macsec replay-protection enable
   ```
   
   # Set the MACsec replay protection window size to 100.
   ```
   [DeviceA-GigabitEthernet1/0/1] macsec replay-protection window-size 100
   ```
   
   # Set the MACsec validation mode to **strict**.
   ```
   [DeviceA-GigabitEthernet1/0/1] macsec validation mode strict
   ```
   
   # Enable MKA on GigabitEthernet 1/0/1.
   ```
   [DeviceA-GigabitEthernet1/0/1] mka enable
   ```
   ```
   [DeviceA-GigabitEthernet1/0/1] quit
   ```

2. Configure Device B:

   # Enter system view.
   ```
   <DeviceB> system-view
   ```
   
   # Enter GigabitEthernet 1/0/1 interface view.
   ```
   [DeviceB] interface gigabitethernet 1/0/1
   ```
   
   # Enable MACsec desire on GigabitEthernet 1/0/1.
   ```
   [DeviceB-GigabitEthernet1/0/1] macsec desire
   ```
# Set the MKA key server priority to 10.
[DeviceB-GigabitEthernet1/0/1] mka priority 10

# Configure the CKN as E9AC and the CAK as 09DB3EF1 in plain text.
[DeviceB-GigabitEthernet1/0/1] mka psk ckn E9AC cak simple 09DB3EF1

# Set the MACsec confidentiality offset to 30 bytes.
[DeviceB-GigabitEthernet1/0/1] macsec confidentiality-offset 30

# Enable MACsec replay protection.
[DeviceB-GigabitEthernet1/0/1] macsec replay-protection enable

# Set the MACsec replay protection window size to 100.
[DeviceB-GigabitEthernet1/0/1] macsec replay-protection window-size 100

# Set the MACsec validation mode to strict.
[DeviceB-GigabitEthernet1/0/1] macsec validation mode strict

# Enable MKA on GigabitEthernet 1/0/1.
[DeviceB-GigabitEthernet1/0/1] mka enable
[DeviceB-GigabitEthernet1/0/1] quit

Verifying the configuration

# Display MACsec information on GigabitEthernet 1/0/1 of Device A.
[DeviceA] display macsec interface gigabitethernet 1/0/1 verbose

Interface GigabitEthernet1/0/1
  Protect frames : Yes
  Replay protection : Enabled
  Replay window size : 100 frames
  Confidentiality offset : 30 bytes
  Validation mode : Strict
  Included SCI : No
  SCI conflict : No
  Cipher suite : GCM-AES-128

Transmit secure channel:
  SCI : 00E0010000A0006
  Elapsed time: 00h:05m:00s
  Current SA : AN 0        PN 1

Receive secure channels:
  SCI : 00E0020000000106
  Elapsed time: 00h:03m:18s
  Current SA : AN 0        LPN 1
  Previous SA : AN N/A      LPN N/A

# Display MKA session information on GigabitEthernet 1/0/1 of Device A.
[DeviceA] display mka session interface gigabitethernet 1/0/1 verbose

Interface GigabitEthernet1/0/1
  Tx-SCI : 00E0010000A0006
  Priority : 5
  Capability: 3
  CKN for participant: E9AC
  Key server : Yes
  MI (MN) : 85E004AF49934720AC5131D3 (182)
  Live peers : 1
  Potential peers : 0
Principal actor       : Yes
MKA session status    : Secured
Confidentiality offset: 30 bytes
Current SAK status    : Rx & Tx
Current SAK AN        : 0
Current SAK KI (KN)   : 85E004AF49934720AC5131D300000003 (3)
Previous SAK status   : N/A
Previous SAK AN       : N/A
Previous SAK KI (KN)  : N/A

Live peer list:
<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Priority</th>
<th>Capability</th>
<th>Rx SCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>12A1677D59DD211AE86A0128</td>
<td>182</td>
<td>10</td>
<td>3</td>
<td>00E0020000000106</td>
</tr>
</tbody>
</table>

# Display MACsec information on GigabitEthernet 1/0/1 of Device B.

[DeviceB] display macsec interface gigabitethernet 1/0/1 verbose

Interface GigabitEthernet1/0/1
Protect frames         : Yes
Replay protection      : Enabled
Replay window size     : 100 frames
Confidentiality offset : 30 bytes
Validation mode        : Strict
Included SCI           : No
SCI conflict           : No
Cipher suite           : GCM-AES-128

Transmit secure channel:
SCI : 00E0020000000106
Elapsed time: 00h:05m:36s
Current SA : AN 0        PN 1

Receive secure channels:
SCI : 00E00100000A0006
Elapsed time: 00h:03m:21s
Current SA : AN 0        LPN 1
Previous SA : AN N/A      LPN N/A

# Display MKA session information on GigabitEthernet 1/0/1 of Device B.

[DeviceB] display mka session interface gigabitethernet 1/0/1 verbose

Interface GigabitEthernet1/0/1
Tx SCI : 00E0020000000106
Priority : 10
Capability: 3
CKN for participant: E9AC
Key server            : No
MI (MN)               : 12A1677D59DD211AE86A0128 (1219)
Live peers            : 1
Potential peers       : 0
Principal actor       : Yes
MKA session status    : Secured
Confidentiality offset: 30 bytes
Current SAK status    : Rx & Tx
Current SAK AN        : 0
Current SAK KI (KN) : 85E004AF49934720AC5131D300000003 (3)
Previous SAK status : N/A
Previous SAK AN : N/A
Previous SAK KI (KN) : N/A
Live peer list:
<table>
<thead>
<tr>
<th>MI</th>
<th>MN</th>
<th>Priority</th>
<th>Capability</th>
<th>Rx-SCI</th>
</tr>
</thead>
<tbody>
<tr>
<td>85E004AF49934720AC5131D3</td>
<td>1216</td>
<td>5</td>
<td>3</td>
<td>00E00100000A0006</td>
</tr>
</tbody>
</table>

Troubleshooting MACsec

Symptom

The devices cannot establish MKA sessions when the following conditions exist:

- The link connecting the devices is up.
- The ports at the ends of the link are MACsec capable.

Analysis

The symptom might occur for the following reasons:

- The ports at the link are not enabled with MKA.
- A port at the link is not configured with a preshared key or configured with a preshared key different from the peer.

Solution

To resolve the problem:

1. Enter interface view.
2. Use the display this command to check the MACsec configuration:
   - If MKA is not enabled on the port, execute the mka enable command.
   - If a preshared key is not configured or the preshared key is different from the peer, use the mka psk command to configure a preshared key. Make sure the preshared key is the same as the preshared key on the peer.
3. If the problem persists, contact Hewlett Packard Enterprise Support.
Configuring ND attack defense

Overview

IPv6 Neighbor Discovery (ND) attack defense is able to identify forged ND messages to prevent ND attacks.

The IPv6 ND protocol does not provide any security mechanisms and is vulnerable to network attacks. As shown in Figure 144, an attacker can send the following forged ICMPv6 messages to perform ND attacks:

- Forged NS/NA/RS messages with an IPv6 address of a victim host. The gateway and other hosts update the ND entry for the victim with incorrect address information. As a result, all packets intended for the victim are sent to the attacking terminal.
- Forged RA messages with the IPv6 address of a victim gateway. As a result, all hosts attached to the victim gateway maintain incorrect IPv6 configuration parameters and ND entries.

Figure 144 ND attack diagram

Feature and software version compatibility

The ND attack defense feature is available in Release 1121 and later.

ND attack defense configuration task list

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Configuring ND attack detection (applicable to access devices)</td>
</tr>
<tr>
<td>(Optional.) Configuring RA guard (applicable to Layer 2 access devices)</td>
</tr>
</tbody>
</table>
Configuring ND attack detection

About ND attack detection

ND attack detection checks incoming ND messages for user validity to prevent spoofing attacks. It is typically configured on access devices.

ND attack detection defines the following types of interfaces:

- **ND trusted interface**—The device directly forwards ND messages or data packets received by ND trusted interfaces. It does not perform user validity check.
- **ND untrusted interface**—The device discards RA and redirect messages received by ND untrusted interfaces. For other types of ND messages received by the ND untrusted interfaces, the device checks the user validity.

ND attack detection compares the source IPv6 address and the source MAC address in an incoming ND message against security entries from other modules.

- If a match is found, the device verifies the user as legal in the receiving VLAN, and it forwards the packet.
- If no match is found, the device verifies the user as illegal, and it discards the ND message.

ND attack detection uses the following security entries for user validity check:

- Static IPv6 source guard binding entries, which are created by using the `ipv6 source binding` command. For information about IPv6 source guard, see "Configuring IP source guard."
- ND snooping entries. For information about ND snooping, see *Layer 3–IP Services Configuration Guide*.
- DHCPv6 snooping entries. For information about DHCPv6 snooping, see *Layer 3–IP Services Configuration Guide*.

Configuration guidelines

When you configure ND attack detection, follow these restrictions and guidelines:

- Make sure one or more of the following features are configured to prevent ND untrusted interfaces from dropping all received ND messages:
  - IPv6 source guard static bindings.
  - DHCPv6 snooping.
  - ND snooping.
- To make the IPv6 source guard static bindings effective for ND attack detection, you must perform the following operations:
  - Specify the `vlan vlan-id` option in the `ipv6 source binding` command.
  - Enable ND attack detection for the same VLAN.

Configuration procedure

To configure ND attack detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>vlan vlan-id</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>ipv6 nd detection enable</td>
<td>By default, ND attack detection is</td>
</tr>
</tbody>
</table>
### Displaying and maintaining ND attack detection

Execute **display** commands in any view and **reset** commands in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display statistics for ND messages dropped by ND attack detection.</td>
<td><code>display ipv6 nd detection statistics [ interface interface-type interface-number ]</code></td>
</tr>
<tr>
<td>Clear ND attack detection statistics.</td>
<td><code>reset ipv6 nd detection statistics [ interface interface-type interface-number ]</code></td>
</tr>
</tbody>
</table>

### ND attack detection configuration example

**Network requirements**

As shown in Figure 145, configure ND attack detection on Device B to check user validity for ND messages from Host A and Host B.

**Figure 145 Network diagram**

![Network Diagram]

Device A

- GE1/0/3
- Vlan-int10
- 10::1/64

Gateway

- GE1/0/1
- GE1/0/2
- GE1/0/3
- Vlan-int10
- 10::1/64

Device B

- ND snooping
- GE1/0/3

VLAN 10

Host A

- 10::5/64
- 0001-0203-0405

Host B

- 10::5/64
- 0001-0203-0607
1. Configure Device A:

   # Create VLAN 10.
   <DeviceA> system-view
   [DeviceA] vlan 10
   [DeviceA-vlan10] quit

   # Configure GigabitEthernet 1/0/3 to trunk VLAN 10.
   [DeviceA] interface gigabitethernet 1/0/3
   [DeviceA-GigabitEthernet1/0/3] port link-type trunk
   [DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 10
   [DeviceA-GigabitEthernet1/0/3] quit

   # Assign IPv6 address 10::1/64 to VLAN-interface 10.
   [DeviceA] interface vlan-interface 10
   [DeviceA-Vlan-interface10] ipv6 address 10::1/64
   [DeviceA-Vlan-interface10] quit

2. Configure Device B:

   # Create VLAN 10.
   <DeviceB> system-view
   [DeviceB] vlan 10
   [DeviceB-vlan10] quit

   # Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to trunk VLAN 10.
   [DeviceB] interface gigabitethernet 1/0/1
   [DeviceB-GigabitEthernet1/0/1] port link-type access
   [DeviceB-GigabitEthernet1/0/1] port access vlan 10
   [DeviceB-GigabitEthernet1/0/1] quit
   [DeviceB] interface gigabitethernet 1/0/2
   [DeviceB-GigabitEthernet1/0/2] port link-type access
   [DeviceB-GigabitEthernet1/0/2] port access vlan 10
   [DeviceB-GigabitEthernet1/0/2] quit
   [DeviceB] interface gigabitethernet 1/0/3
   [DeviceB-GigabitEthernet1/0/3] port link-type trunk
   [DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 10
   [DeviceB-GigabitEthernet1/0/3] quit

   # Enable ND attack detection for VLAN 10.
   [DeviceB] vlan 10
   [DeviceB-vlan10] ipv6 nd detection enable

   # Enable ND snooping for IPv6 global unicast addresses and ND snooping for IPv6 link-local addresses in VLAN 10.
   [DeviceB-vlan10] ipv6 nd snooping enable global
   [DeviceB-vlan10] ipv6 nd snooping enable link-local
   [DeviceB-vlan10] quit

   # Configure GigabitEthernet 1/0/3 as ND trusted interface.
   [DeviceB] interface gigabitethernet 1/0/3
   [DeviceB-GigabitEthernet1/0/3] ipv6 nd detection trust
Verifying the configuration

Verify that Device B inspects all ND messages received by GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 based on the ND snooping entries. (Details not shown.)

Configuring RA guard

About RA guard

RA guard allows Layer 2 access devices to analyze and block unwanted and forged RA messages. Upon receiving an RA message, the device makes the forwarding or dropping decision based on the role of the attached device or the RA guard policy.

1. If the role of the device attached to the receiving port is router, the device forwards the RA message. If the role is host, the device drops the RA message.
2. If no attached device role is set, the device uses the RA guard policy applied to the VLAN of the receiving port to match the RA message.
   - If the policy does not contain match criteria, the policy will not take effect and the device forwards the RA message.
   - If the RA message content matches every criterion in the policy, the device forwards the message. Otherwise, the device drops the message.

Specifying the role of the attached device

Make sure your setting is consistent with the type of the attached device. If you are not aware of the device type, do not specify a role for the device.

To specify the role of the attached device:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter Layer 2 Ethernet or aggregate interface view.</td>
<td>interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the role of the device attached to the port.</td>
<td>ipv6 nd raguard role { host</td>
</tr>
</tbody>
</table>

Configuring and applying an RA guard policy

Configure an RA guard policy if you do not specify a role for the attached device or if you want to filter the RA messages sent by a router.

To configure and apply an RA guard policy:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an RA guard policy and enter its view.</td>
<td>ipv6 nd raguard policy policy-name</td>
</tr>
<tr>
<td>3.</td>
<td>Specify an ACL match</td>
<td>if-match acl</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>criterion.</td>
<td>{ ipv6-acl-number</td>
<td>name ipv6-acl-name }</td>
</tr>
<tr>
<td>4. Specify a prefix match criterion.</td>
<td>if-match prefix acl { ipv6-acl-number</td>
<td>name ipv6-acl-name }</td>
</tr>
<tr>
<td>5. Specify a router preference match criterion.</td>
<td>if-match router-preference maximum { high</td>
<td>low</td>
</tr>
<tr>
<td>7. Specify an O flag match criterion.</td>
<td>if-match autoconfig other-flag { off</td>
<td>on }</td>
</tr>
<tr>
<td>8. Specify a maximum or minimum hop limit match criterion.</td>
<td>if-match hop-limit { maximum</td>
<td>minimum } limit</td>
</tr>
<tr>
<td>9. Quit RA guard policy view.</td>
<td>quit</td>
<td>N/A</td>
</tr>
<tr>
<td>10. Enter VLAN view.</td>
<td>vlan vlan-number</td>
<td>N/A</td>
</tr>
<tr>
<td>11. Apply an RA guard policy to the VLAN.</td>
<td>ipv6 nd raguard apply policy [ policy-name ]</td>
<td>By default, no RA guard policy is applied to the VLAN.</td>
</tr>
</tbody>
</table>

### Enabling the RA guard logging feature

This feature allows a device to generate logs when it detects forged RA messages. Each log records the following information:

- Name of the interface that received the forged RA message.
- Source IP address of the forged RA message.
- Number of RA messages dropped on the interface.

The RA guard logging feature sends the log messages to the information center. The information center can then output log messages from different source modules to different destinations. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

To enable the RA guard logging feature:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable the RA guard logging feature.</td>
<td>ipv6 nd raguard log enable</td>
<td>By default, the RA guard logging feature is disabled.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining RA guard

Execute **display** commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the RA guard policy configuration.</td>
<td>display ipv6 nd raguard policy [ policy-name ]</td>
</tr>
<tr>
<td>Display RA guard statistics.</td>
<td>display ipv6 nd raguard statistics [ interface interface-type ]</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Clear RA guard statistics.</td>
<td>reset ipv6 nd raguard statistics [ interface interface-type interface-number ]</td>
</tr>
</tbody>
</table>

**RA guard configuration example**

**Network requirements**

As shown in Figure 146, GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 of Device B are in VLAN 10.

Configure RA guard on Device B to filter forged and unwanted RA messages.

- Configure an RA policy in VLAN 10 for GigabitEthernet 1/0/2 to filter all RA messages received from the unknown device.
- Specify **host** as the role of the host. All RA messages received on GigabitEthernet 1/0/1 are dropped.
- Specify **router** as the role of the Device A. All RA messages received on GigabitEthernet 1/0/3 are forwarded.

**Figure 146 Network diagram**

**Configuration procedure**

1. Create an RA guard policy named **policy1**.
   
   ```bash
   <DeviceB> system-view
   [DeviceB] ipv6 nd raguard policy policy1
   ```

2. Set the maximum router preference to **high** for the RA guard policy.
   
   ```bash
   [DeviceB-raguard-policy-policy1] if-match router-preference maximum high
   ```

3. Specify **on** as the M flag match criterion for the RA guard policy.
   
   ```bash
   [DeviceB-raguard-policy-policy1] if-match autoconfig managed-address-flag on
   ```

4. Specify **on** as the O flag match criterion for the RA guard policy.
   
   ```bash
   [DeviceB-raguard-policy-policy1] if-match autoconfig other-flag on
   ```

5. Set the maximum advertised hop limit to 120 for the RA guard policy.
   
   ```bash
   [DeviceB-raguard-policy-policy1] if-match hop-limit maximum 120
   ```

6. Set the minimum advertised hop limit to 100 for the RA guard policy.
   
   ```bash
   [DeviceB-raguard-policy-policy1] if-match hop-limit minimum 100
   ```

   ```bash
   [DeviceB-raguard-policy-policy1] quit
   ```
# Assign GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to VLAN 10.

[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type access
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit

[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type access
[DeviceB-GigabitEthernet1/0/2] port access vlan 10
[DeviceB-GigabitEthernet1/0/2] quit

# Configure GigabitEthernet 1/0/3 to trunk VLAN 10.

[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 10
[DeviceB-GigabitEthernet1/0/3] quit

# Apply the RA guard policy policy1 to VLAN 10.

[DeviceB] vlan 10
[DeviceB-vlan10] ipv6 nd raguard apply policy policy1
[DeviceB-vlan10] quit

# Specify host as the role of the device attached to GigabitEthernet 1/0/1.

[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipv6 nd raguard role host
[DeviceB-GigabitEthernet1/0/1] quit

# Specify router as the role of the device attached to GigabitEthernet 1/0/3.

[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] ipv6 nd raguard role router
[DeviceB-GigabitEthernet1/0/3] quit

Verifying the configuration

# Verify that the device forwards or drops RA messages received on GigabitEthernet 1/0/2 based on the RA guard policy. (Details not shown.)

# Verify that the device drops RA messages received on GigabitEthernet 1/0/1. (Details not shown.)

# Verify that the device forwards RA messages received on GigabitEthernet 1/0/3 to other ports in VLAN 10. (Details not shown.)
Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Command conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boldface</td>
<td>Bold text represents commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td>Italic</td>
<td>Italic text represents arguments that you replace with actual values.</td>
</tr>
<tr>
<td>[]</td>
<td>Square brackets enclose syntax choices (keywords or arguments) that are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>&amp;&lt;1-n&gt;</td>
<td>The argument or keyword and argument combination before the ampersand (&amp;) sign can be entered 1 to n times.</td>
</tr>
<tr>
<td>#</td>
<td>A line that starts with a pound (#) sign is comments.</td>
</tr>
</tbody>
</table>

GUI conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boldface</td>
<td>Window names, button names, field names, and menu items are in Boldface. For example, the New User window opens; click OK.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Multi-level menus are separated by angle brackets. For example, File &gt; Create &gt; Folder.</td>
</tr>
</tbody>
</table>

Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>▼ WARNING!</td>
<td>An alert that calls attention to important information that if not understood or followed can result in personal injury.</td>
</tr>
<tr>
<td>▼ CAUTION:</td>
<td>An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.</td>
</tr>
<tr>
<td>☑ IMPORTANT:</td>
<td>An alert that calls attention to essential information.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
<tr>
<td>☦ TIP:</td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>
# Network topology icons

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="network_icon_1.png" alt="icon" /></td>
<td>Represents a generic network device, such as a router, switch, or firewall.</td>
</tr>
<tr>
<td><img src="network_icon_2.png" alt="icon" /></td>
<td>Represents a routing-capable device, such as a router or Layer 3 switch.</td>
</tr>
<tr>
<td><img src="network_icon_3.png" alt="icon" /></td>
<td>Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.</td>
</tr>
<tr>
<td><img src="network_icon_4.png" alt="icon" /></td>
<td>Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.</td>
</tr>
<tr>
<td><img src="network_icon_5.png" alt="icon" /></td>
<td>Represents an access point.</td>
</tr>
<tr>
<td><img src="network_icon_6.png" alt="icon" /></td>
<td>Represents a wireless terminator unit.</td>
</tr>
<tr>
<td><img src="network_icon_7.png" alt="icon" /></td>
<td>Represents a wireless terminator.</td>
</tr>
<tr>
<td><img src="network_icon_8.png" alt="icon" /></td>
<td>Represents a mesh access point.</td>
</tr>
<tr>
<td><img src="network_icon_9.png" alt="icon" /></td>
<td>Represents omnidirectional signals.</td>
</tr>
<tr>
<td><img src="network_icon_10.png" alt="icon" /></td>
<td>Represents directional signals.</td>
</tr>
<tr>
<td><img src="network_icon_11.png" alt="icon" /></td>
<td>Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.</td>
</tr>
<tr>
<td><img src="network_icon_12.png" alt="icon" /></td>
<td>Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.</td>
</tr>
</tbody>
</table>
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website: www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website: www.hpe.com/support/hpesc

Information to collect
- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center Get connected with updates page: www.hpe.com/support/e-updates
  - Software Depot website: www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page: www.hpe.com/support/AccessToSupportMaterials

**IMPORTANT:**
Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.
Websites

<table>
<thead>
<tr>
<th>Website</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking websites</td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library for Networking</td>
<td><a href="http://www.hpe.com/networking/resourcefinder">www.hpe.com/networking/resourcefinder</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking website</td>
<td><a href="http://www.hpe.com/info/networking">www.hpe.com/info/networking</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise My Networking website</td>
<td><a href="http://www.hpe.com/networking/support">www.hpe.com/networking/support</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking Warranty</td>
<td><a href="http://www.hpe.com/networking/warranty">www.hpe.com/networking/warranty</a></td>
</tr>
<tr>
<td>General websites</td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library</td>
<td><a href="http://www.hpe.com/info/enterprise/docs">www.hpe.com/info/enterprise/docs</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Center</td>
<td><a href="http://www.hpe.com/support/hpesc">www.hpe.com/support/hpesc</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Services Central</td>
<td>ssc.hpe.com/portal/site/ssc/</td>
</tr>
<tr>
<td>Contact Hewlett Packard Enterprise Worldwide</td>
<td><a href="http://www.hpe.com/assistance">www.hpe.com/assistance</a></td>
</tr>
<tr>
<td>Subscription Service/Support Alerts</td>
<td><a href="http://www.hpe.com/support/e-updates">www.hpe.com/support/e-updates</a></td>
</tr>
<tr>
<td>Software Depot</td>
<td><a href="http://www.hpe.com/support/softwaredepot">www.hpe.com/support/softwaredepot</a></td>
</tr>
<tr>
<td>Customer Self Repair (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/support/selfrepair">www.hpe.com/support/selfrepair</a></td>
</tr>
<tr>
<td>Insight Remote Support (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/info/insightremotesupport/docs">www.hpe.com/info/insightremotesupport/docs</a></td>
</tr>
</tbody>
</table>

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website: www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website: www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,
part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
Index

Numerics

3DES
security IPsec encryption algorithm, 262

802
MACsec configuration, 461, 465, 470
802.1X, 64, See also under 802
access control method, 82
ACL assignment configuration, 98
architecture, 64
authentication, 68
authentication (access device initiated), 67
authentication (client initiated), 67
authentication attempts max number for MAC authenticated users, 83
authentication configuration, 94
authentication initiation, 67
authentication request attempts max, 83
authentication timeout timers, 83
authentication trigger, 85
authentication+ACL assignment, 79
authentication+EAD assistant feature, 79
authentication+user profile assignment, 79
Auth-Fail VLAN, 75
Auth-Fail VLAN configuration, 89
authorization VLAN, 72
authorization VLAN configuration, 96
basic configuration, 94
concurrent port users max, 82
configuration, 72, 80
controlled/uncontrolled port, 64
critical VLAN, 76, 91
critical VLAN configuration, 90
critical voice VLAN, 78
critical voice VLAN enable, 91
display, 93
EAD assistant, 100
EAD assistant configuration, 93
EAP over RADIUS, 66
EAP packet format, 65
EAP relay authentication, 69
EAP relay enable, 81
EAP relay/termination authentication, 68
EAP termination enable, 81
EAP termination mode authentication, 70
EAP-Message attribute, 66
EAPOL packet format, 66
EAP-Success packets sending, 91
enable, 80
feature cooperation, 79
guest VLAN, 74
guest VLAN assignment delay, 88
guest VLAN configuration, 87, 96
MAC authentication delay, 110
MAC-based access control, 72
maintain, 93
mandatory port authentication domain, 86
online user handshake, 84
overview, 64
packet format, 65
periodic online user reauthentication, 87
port authorization state, 82
port authorization status, 64
port security authentication control mode, 185
port security client
macAddressElseUserLoginSecure, 201
port security client userLoginWithOUI, 198
port security configuration, 185, 188, 196
port security features, 190
port security intrusion protection, 191
port security MAC address autoLearn, 196
port security MAC move, 193
port security MAC+802.1X authentication, 187
port security mode, 189
port security NTK, 190
port-based access control, 72
quiet timer, 86
RADIUS Message-Authentication attribute, 67
related protocols, 65
security user profile configuration, 454
supported domain name delimiters, 92
troubleshoot, 102
troubleshoot EAD assistant Web browser users, 102
VLAN manipulation, 72

A
AAA
concurrent login user max, 48
configuration, 1, 17, 49
device implementation, 11
display, 49
displaying local users/user groups, 22
FIPS compliance, 16
HWTACACS accounting server, 35
HWTACACS authentication server, 34
HWTACACS authorization server, 34
HWTACACS display, 39
HWTACACS implementation, 6
HWTACACS maintain, 39
HWTACACS outgoing packet source IP address, 37
HWTACACS scheme, 33
HWTACACS scheme creation, 34
HWTACACS scheme VPN, 36
HWTACACS server SSH user, 49
HWTACACS shared keys, 36
HWTACACS timer set, 38
HWTACACS traffic statistics units, 37
HWTACACS username format, 37
HWTACACS/RADIUS differences, 7
ISP domain accounting method, 47
ISP domain attribute configuration, 44
ISP domain authentication method, 44
ISP domain authorization method, 45
ISP domain creation, 43
ISP domain method, 43
LDAP administrator attribute, 41
LDAP authentication server, 42
LDAP display, 42
LDAP implementation, 9
LDAP scheme, 40
LDAP scheme creation, 42
LDAP server creation, 40
LDAP server IP address, 40
LDAP server SSH user authentication, 56
LDAP user attribute, 41
LDAP versions, 40
local user attribute, 19
local user configuration, 18
methods, 12
MPLS L3VPN implementation, 13
NAS-ID profile configuration, 48
protocols and standards, 13
RADIUS accounting server parameters, 25
RADIUS accounting-on configuration, 31
RADIUS attributes, 14
RADIUS authentication server, 24
RADIUS display, 33
RADIUS implementation, 2
RADIUS maintain, 33
RADIUS request transmission attempts max, 27
RADIUS scheme, 22
RADIUS scheme creation, 23
RADIUS scheme VPN, 26
RADIUS security policy server IP address, 32
RADIUS server load sharing, 29
RADIUS server SSH user authentication+authorization, 52
RADIUS server status, 28
RADIUS session-control, 48
RADIUS shared keys, 26
RADIUS SNMP notification, 32
RADIUS timer set, 30
RADIUS traffic statistics units, 26
RADIUS username format, 26
scheme configuration, 18
SS user local authentication+HWTACACS authorization+RADIUS accounting, 50
troubleshoot HWTACACS, 62
troubleshoot LDAP, 62
troubleshoot LDAP authentication failure, 62
troubleshoot RADIUS, 61
troubleshoot RADIUS accounting error, 62
troubleshoot RADIUS authentication failure, 61
troubleshoot RADIUS packet delivery failure, 61
user group attribute, 21
user management by ISP domains, 11
user management by user access types, 11
access control
direct portal authentication configuration (local portal Web server), 144, 179
security portal authentication, 129
security portal authentication configuration, 123, 145
security portal authentication cross-subnet, 156
security portal authentication direct, 145
security portal authentication extended cross-subnet, 166
security portal authentication extended direct, 159
security portal authentication extended re-DHCP, 162
security portal authentication re-DHCP, 153
security portal authentication server detection+user synchronization, 169
accessing
security portal authentication device access, 124
account idle time (password control), 208
accounting
AAA configuration, 1, 17, 49
AAA ISP domain accounting method, 47
AAA RADIUS accounting server parameters, 25
AAA RADIUS accounting-on, 31
AAA SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
ACL
- 802.1X authentication+ACL assignment, 79
- 802.1X+ACL assignment configuration, 98
- MAC authentication ACL assignment, 105, 119
- security IPsec ACL, 265
- security IPsec ACL de-encapsulated packet check, 273
- security IPsec ACL rule keywords, 265
- security IPsec ACL-based implementation, 262, 264
- security IPsec ACL-based tunnel establishment, 263
- security IPsec mirror image ACLs, 265
- security IPsec non-mirror image ACLs, 265
- SSH management parameters, 336
active
- ARP active acknowledgement, 417
- security portal authentication type, 123
address
- Address Resolution Protocol. Use ARP uRPF configuration, 438, 442
- uRPF enable, 441
AES
- security IPsec encryption algorithm, 262
AH
- IPsec security protocol 51, 260
alert protocol (SSL), 393
algorithm
- security IPsec authentication, 262
- security IPsec encryption (3DES), 262
- security IPsec encryption (AES), 262
- security IPsec encryption (DES), 262
- security IPsec IKE DH algorithm, 292
- SSH negotiation, 329
anti-replay
- IPsec anti-replay window and sequence number synchronization, 274
anti-replay (IPsec), 274
any authentication (SSH), 329
application
- security IPsec application-based implementation, 263
- security IPsec application-based tunnel establishment, 263
- uRPF network, 441
applying
- interface NAS ID profile, 141
- MACsec MKA policy, 469
- port security NAS-ID profile, 194
- security IPsec policy to interface, 273
architecture
- 802.1X, 64
- PKI, 227
ARP
- attack protection. See ARP attack protection
- MFF configuration, 431, 433, 435
- MFF configuration (manual-mode in ring network), 436
- MFF configuration (manual-mode in tree network), 435
- scanning configuration restrictions, 426
ARP attack protection
- active acknowledgement, 417
- ARP attack detection display, 423
- ARP attack detection maintain, 423
- authorized ARP configuration, 417
- authorized ARP configuration (DHCP relay agent), 419
- authorized ARP configuration (DHCP server), 418
- configuration (user+packet validity check), 423
detection configuration, 420
- filtering configuration, 428, 429
- fixed ARP configuration, 426
gateway protection, 427, 428
- logging enable, 422
- packet rate limit configuration, 413
- packet source MAC consistency check, 416
- packet validity check configuration, 421
- restricted forwarding, 422
- restricted forwarding configuration, 424
- scanning configuration, 426
- source MAC-based attack detection, 414, 415
- source MAC-based detection display, 415
- unresolvable IP attack, 411, 413
- unresolvable IP attack blackhole routing, 412
- unresolvable IP attack protection display, 412
- unresolvable IP attack source suppression, 412
- user validity check, 420
assigning
- 802.1X authentication+ACL assignment, 79
- 802.1X authentication+user profile assignment, 79
- MAC authentication ACL, 119
assignment
- 802.1X guest VLAN assignment delay, 88
associating
- MACsec connectivity association (CA), 461
- MACsec connectivity association key (CAK), 461
- MACsec secure association (SA), 461
- MACsec secure association key (SAK), 461
attack
ARP attack protection configuration, 411
attack D&P configuration, 460
TCP fragment attack prevention configuration, 460
attack detection and prevention. See attack D&P
attacking detection and prevention. See attack D&P
attribute
802.1X RADIUS EAP-Message, 66
802.1X RADIUS Message-Authentication, 67
AAA HWTACACS scheme, 33
AAA ISP domain attribute, 44
AAA LDAP administrator attribute, 41
AAA LDAP scheme, 40
AAA LDAP user attribute, 41
AAA local user, 18
AAA local user attribute, 19
AAA RADIUS, 14
AAA RADIUS common standard attributes, 14
AAA RADIUS extended attributes, 6
AAA RADIUS H3C proprietary attributes, 15
AAA RADIUS Login-Service attribute check method, 32
AAA RADIUS scheme, 22
AAA scheme, 18
AAA user group attribute, 21
authenticating
802.1X access device initiated authentication, 67
802.1X authentication, 68
802.1X authentication attempts max number for MAC authenticated users, 83
802.1X authentication request attempts max, 83
802.1X authentication trigger, 85
802.1X client-initiated, 67
802.1X EAP over RADIUS, 66
802.1X EAP relay authentication, 69
802.1X EAP relay enable, 81
802.1X EAP relay/termination, 68
802.1X EAP termination enable, 81
802.1X EAP termination mode authentication, 70
802.1X initiation, 67
802.1X mandatory port authentication domain, 86
802.1X overview, 64
802.1X periodic online user reauthentication, 87
802.1X RADIUS Message-Authentication attribute, 67
802.1X timeout timers, 83
802.1X VLAN manipulation, 72
AAA configuration, 1, 17, 49
AAA ISP domain authentication method, 44
AAA LDAP authentication, 9
AAA LDAP server SSH user authentication, 56
AAA RADIUS server SSH user authentication+authorization, 52
AAA RADIUS user authentication methods, 2
AAA SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
IPsec IKEv2+pre-shared key authentication, 318
IPsec IKEv2+RSA signature authentication, 321
MAC authentication, 103, 107, 115
MAC authentication (local), 115
MAC authentication (RADIUS-based), 117
MAC authentication VLAN assignment, 104
MAC local authentication method, 103
MAC RADIUS authentication method, 103
periodic MAC reauthentication, 106
port security authentication modes, 185
port security client macAddressElseUserLoginSecure, 201
port security client userLoginWithOUI, 198
port security configuration, 185, 188, 196
port security MAC address autoLearn, 196
security IPsec, 262
security IPsec authentication algorithms, 262
security IPsec Authentication Header. Use AH
security IPsec configuration, 259, 280
security IPsec Encapsulating Security Payload. Use ESP
security IPsec IKE (main mode/pre-shared key authentication), 301
security IPsec IKE DSA signature authentication, 291
security IPsec IKE pre-shared key authentication, 291
security IPsec IKE RSA signature authentication, 291
security IPsec RIPIng, 285
security IPsec tunnel for IPv4 packets (IKE-based), 283
security IPsec tunnel for IPv4 packets (manual), 280
security password control, 209, 213
security password control configuration, 206
security portal authentication (cross-subnet for MPLS L3VPN), 177
security portal authentication client, 124
security portal authentication server, 124
security user profile configuration, 454
SSH configuration, 328
SSH methods, 329
SSH SCP file transfer+password authentication, 381
SSH Secure Telnet client configuration (password authentication-enabled), 362
SSH Secure Telnet client configuration (publickey authentication-enabled), 365
SSH Secure Telnet server configuration (password authentication-enabled), 354
SSH Secure Telnet server configuration (publickey authentication-enabled), 356
SSH server configuration, 331
SSH SFTP client configuration (publickey authentication-enabled), 374
SSH SFTP server configuration (password authentication-enabled), 372
SSL services, 393
authentication
creating user profile, 454
Authentication, Authorization, and Accounting. Use AAA
Auth-Fail VLAN
802.1X authentication, 75
802.1X configuration, 89
authorization VLAN
802.1X assignment, 73
802.1X configuration, 96
802.1X supported, 72
802.1X unsupported, 73
MAC authentication, 104
authorized ARP
configuration, 417
configuration configuration (DHCP relay agent), 419
configuration configuration (DHCP server), 418
authorizing
802.1X authorization VLAN, 72
802.1X port authorization state, 82
802.1X port authorization status, 64
802.1X port authorized-force state, 82
802.1X port auto state, 82
802.1X port unauthorized-force state, 82
AAA configuration, 1, 17, 49
AAA ISP domain authorization method, 45
AAA LDAP authorization, 9
AAA RADIUS server load sharing, 29
AAA RADIUS server SSH user authentication+authorization, 52
AAA RADIUS session-control, 48
AAA SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
MAC authentication authorization VLAN, 104
port security authorization-fail-offline feature, 194
port security server authorization information ignore, 193
auto
FIPS mode (automatic reboot), 445
FIPS mode exit (automatic reboot), 447, 452
PKI certificate request (automatic), 233
port security MAC address autoLearn, 196
B
BAS-IP
security portal authentication BAS-IP, 140
binding
IP source guard (IPSG) dynamic binding, 401
IP source guard (IPSG) static binding, 400
IPv4 source guard (IPv4SG) static binding configuration, 402
IPv6 source guard (IPv6SG) static binding configuration, 404
security IPsec source interface to policy, 275
blackhole
ARP attack protection blackhole routing (unresolvable IP attack), 412
C
CA
PKI architecture, 227
PKI CA policy, 227
PKI certificate, 226
PKI certificate export, 237
PKI certificate obtain, 234
PKI certificate removal, 237
PKI certificate request, 232
PKI certificate request (automatic), 233
PKI certificate request (manual), 233
PKI certificate request abort, 234
PKI certificate verification, 235
PKI CRL, 226
PKI domain configuration, 230
PKI entity configuration, 229
PKI OpenCA server certificate request, 245
PKI RSA Keon CA server certificate request, 239
PKI storage path, 236
PKI Windows 2003 CA server certificate request, 242
troubleshooting PKI CA certificate import failure, 256
troubleshooting PKI CA certificate obtain failure, 254
CA (MACsec), 461
CAK (MACsec), 461
CAR
  user profile configuration, 455
certificate
  authority. Use CA
  PKI certificate verification (CRL checking), 235
  PKI certificate verification (w/o CRL checking), 236
revocation list. Use CRL
challenging
  IPsec IKEv2 cookie challenge, 317
changing
  SSL change cipher spec protocol, 393
CHAP/PAP authentication
  direct/cross-subnet portal authentication process, 127
  re-DHCP portal authentication process, 128
checking
  MACsec integrity check, 461
  PKI certificate verification (CRL checking), 235
  PKI certificate verification (w/o CRL checking), 236
security IPsec ACL de-encapsulated packet check, 273
  uRPF loose check mode, 438
  uRPF strict check mode, 438
classifying
  security IPsec QoS pre-classify enable, 276
clearing
  security IPsec packet DF bit clear, 276
client
  802.1X authentication, 68
  802.1X authentication (access device initiated), 67
  802.1X authentication (client-initiated), 67
  802.1X authentication client timeout timer, 83
  802.1X authentication configuration, 94
  802.1X authentication initiation, 67
  802.1X authorization VLAN configuration, 96
  802.1X basic configuration, 94
  802.1X configuration, 72, 80
  802.1X guest VLAN configuration, 96
  802.1X+ACL assignment configuration, 98
MACsec (client-oriented), 470
MACsec operation (client-oriented), 462
security portal authentication, 124
security portal authentication system components, 123
SSL client policy configuration, 397
command
  AAA command accounting method, 12
  AAA command authorization method, 12
comparing
  802.1X EAP relay/termination authentication, 68
  complexity checking (password control), 206
  composition checking (password control), 206
  conditional self-test, 448
confidentiality
  MACsec confidentiality offset, 467
configuring
  802.1X Auth-Fail VLAN, 75, 89
  802.1X authorization VLAN, 96
  802.1X critical VLAN, 76, 90
  802.1X critical voice VLAN, 78
  802.1X EAD assistant, 100
  802.1X guest VLAN, 96
  802.1X+ACL assignment, 98
  AAA HWTACACS schemes, 33
  AAA RADIUS Login-Service attribute check method, 32
  ARP filtering, 428, 429
  ARP gateway protection, 428
crypto gateway protection, 428
  crypto engine, 443
  FIPS, 444
  IPsec IKEv2+pre-shared key authentication, 318
  IPsec IKEv2+RSA signature authentication, 321
IPv6 ND attack defense RA guard, 483
MAC authentication, 103, 107
MACsec, 465, 470
MACsec (client-oriented), 470
MACsec (device-oriented), 473
MFF, 431, 433
MFF (manual-mode in tree network), 435
NETCONF-over-SSH client user line, 334
NETCONF-over-SSH+password authentication, 390
peer host public key, 220
PKI, 226
Secure Telnet client user line, 334
security IPsec, 259, 280
  security IPsec IPv6 routing protocol profile, 278
security IPsec IPv6 routing protocols, 277
security IPsec packet DF bit, 276
security IPsec policy (IKE-based), 269
security IPsec SNMP notification, 279
security IPsec transform set, 265
security IPsec tunnel for IPv4 packets (manual), 280
security SSH SCP, 381
security SSH SCP (Suite B), 383
SSH, 328
SSH client host public key, 334
SSH SCP file+password authentication, 381
SSH Secure Telnet (128-bit Suite B), 367
SSH Secure Telnet client (password authentication-enabled), 362
SSH Secure Telnet client (publickey authentication-enabled), 365
SSH Secure Telnet server (publickey authentication-enabled), 356
SSH SFTP, 371
SSH SFTP (192-bit Suite B), 377
SSH SFTP client (publickey authentication-enabled), 374
SSH SFTP server (password authentication-enabled), 372
uRPF, 442

Configuring
802.1X critical VLAN, 91
Configuring
802.1X, 72, 80
802.1X authentication, 94
802.1X authentication trigger, 85
802.1X basics, 94
802.1X EAD assistant, 93
802.1X guest VLAN, 74, 87
802.1X online user handshake, 84
AAA, 1, 17, 49
AAA HWTACACS server SSH user, 49
AAA ISP domain accounting method, 47
AAA ISP domain attribute, 44
AAA ISP domain authentication method, 44
AAA ISP domain authorization method, 45
AAA ISP domain method, 43
AAA LDAP administrator attributes, 41
AAA LDAP scheme, 40
AAA LDAP server IP address, 40
AAA LDAP server SSH user authentication, 56
AAA LDAP user attributes, 41
AAA local user, 18
AAA local user attributes, 19
AAA NAS-ID profile, 48
AAA RADIUS accounting-on, 31
AAA RADIUS scheme, 22
AAA RADIUS security policy server IP address, 32
AAA RADIUS server SSH user authentication+authorization, 52
AAA RADIUS server status detection test profile, 23
AAA scheme, 18
AAA SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
AAA user group attributes, 21
ARP active acknowledgement, 417
ARP attack detection, 420
ARP attack detection (source MAC-based), 414, 415
ARP attack detection (user+packet validity check), 423
ARP attack detection packet validity check, 421
ARP attack detection restricted forwarding, 422, 424
ARP attack detection user validity check, 420
ARP attack protection, 411
ARP attack protection (unresolvable IP attack), 411, 413
ARP attack protection blackhole routing (unresolvable IP attack), 412
ARP attack protection source suppression (unresolvable IP attack), 412
ARP gateway protection, 427
ARP packet rate limit, 413
ARP packet source MAC consistency check, 416
ARP scanning, 426
attack D&P, 460
authorized ARP, 417
authorized ARP (DHCP relay agent), 419
authorized ARP (DHCP server), 418
direct portal authentication (local portal Web server), 179
direct security portal authentication (local portal Web server), 144
dynamic IPv4 source guard (IPv4SG)+DHCP relay agent, 407
dynamic IPv4 source guard (IPv4SG)+DHCP snooping, 406
dynamic IPv6 source guard (IPv6SG)+DHCPv6 snooping, 409
FIPS, 449
FIPS mode, 445
fixed ARP, 426
IP source guard (IPSG), 400, 401, 405
IPsec IKEv2, 309, 311, 318
IPsec IKEv2 DPD, 317
IPsec IKEv2 global parameters, 317
IPsec IKEv2 keychain, 316
IPsec IKEv2 NAT keepalive, 317
security portal authentication server detection, 137
security portal authentication server detection+user synchronization, 169
security portal authentication source subnet, 133
security portal authentication user online detection, 136
security portal authentication user synchronization, 138
security portal authentication Web server, 130
security portal authentication Web server detection, 138
security user profile, 454
SSH device as Secure Telnet client, 338
SSH device as server, 331
SSH device as SFTP client, 342
SSH management parameters, 336
SSH SCP client device, 348
SSH Secure Telnet, 353
SSH Secure Telnet server (password authentication-enabled), 354
SSH user, 335
SSH2 algorithms (encryption), 352
SSH2 algorithms (key exchange), 352
SSH2 algorithms (MAC), 353
SSH2 algorithms (public key), 352
SSL, 393, 394
SSL client policy, 397
SSL server policy, 394
static IPv4 source guard (IPv4SG), 405
static IPv6 source guard (IPv6SG), 408
TCP fragment attack prevention, 460
uRPF, 438
user profile, 455
user profile parameters, 455
configuring and applying
IPv6 ND attack defense RA guard policy, 481
connecting
MACsec connectivity association (CA), 461
MACsec connectivity association key (CAK), 461
consistency check (ARP attack protection), 416
controlling
802.1X controlled/uncontrolled port, 64
AAA RADIUS session-control, 48
port security MAC address learning, 186
security portal authentication user access, 132
cookie
IPsec IKEv2 cookie challenge, 310, 317
copying
security IPsec packet DF bit copy, 276
creating
AAA HWTACACS scheme, 34
AAA ISP domain, 43
AAA LDAP scheme, 42
AAA RADIUS scheme, 23
local key pair, 217
security LDAP server, 40
user profile, 454
critical VLAN
802.1X authentication, 76
802.1X configuration, 90
MAC authentication, 105
MAC authentication configuration, 112
critical voice VLAN
802.1X authentication, 78
802.1X enable, 91
MAC authentication enable, 113
CRL
PKI, 226
PKI architecture, 227
PKI CA policy, 227
PKI certificate export, 237
PKI certificate removal, 237
PKI certificate-based access control policy, 238
PKI storage path, 236
troubleshooting PKI CRL obtain failure, 255
cross-subnet
portal authentication, 156
portal authentication (MPLS L3VPN), 177
portal authentication mode, 126, 127
crypto engine
configuration, 443
displaying, 443
maintaining, 443
cryptography
FIPS self-test, 447
customizing
portal authentication local portal Web server page customization, 125
portal authentication pages, 142, 142
D
data
MACsec configuration, 461, 465, 470
MACsec configuration (client-oriented), 470
MACsec configuration (device-oriented), 473
SSL configuration, 393, 394
data encryption
PKI configuration, 226, 229, 239
delay
  802.1X guest VLAN assignment delay, 88
delaying
  MAC authentication delay, 110
delimiter (802.1X domain name), 92
DES
  security IPsec encryption algorithm, 262
desire
  MACsec enable, 465
destination
  security portal authentication portal-free rule, 132
  security portal authentication subnet, 134
destroying
  local key pair, 220
detecting
  AAA RADIUS server status detection test profile, 23
  ARP attack detection (source MAC-based), 414, 415
  ARP attack detection configuration, 420
  MAC authentication offline detection enable, 114, 114
  security portal authentication detection features, 136
  security portal authentication server, 137
  security portal authentication server detection+user synchronization, 169
  security portal authentication user online detection, 136
  security portal authentication user synchronization, 138
  security portal authentication Web server, 138
device
  802.1X authentication, 68
  802.1X authentication configuration, 94
  802.1X authentication initiation, 67
  802.1X authorization VLAN configuration, 96
  802.1X basic configuration, 94
  802.1X configuration, 72, 80
  802.1X EAD assistant, 93
  802.1X guest VLAN configuration, 96
  802.1X+ACL assignment configuration, 98
  attack D&P configuration, 460
  authorized ARP configuration (DHCP server), 418
  creating user profile, 454
  crypto engine configuration, 443
direct portal authentication configuration (local portal Web server), 179
IPv6 ND attack defense device role, 481
MAC authentication, 107, 115
MAC authentication (local), 115
MAC authentication (RADIUS-based), 117
MAC authentication ACL assignment, 119
MAC authentication configuration, 103
MACsec (device-oriented), 473
MACsec operation (device-oriented), 462
MFF server IP address, 434
NETCONF-over-SSH+password authentication configuration, 390
port security server authorization information ignore, 193
security password server authorization information ignore, 209, 213
security password control configuration, 206
security password control global parameters, 210
security password control local user parameters, 212
security password control user group parameters, 211
security password setting, 206
security portal authentication AAA server, 124
security portal authentication client, 124
security portal authentication device access, 124
security portal authentication policy server, 124
security portal authentication server, 124
security portal authentication Web server, 124
security super password control parameters, 212
security user profile configuration, 454
SSH SCP client, 348
SSH SCP file transfer+password authentication, 381
SSH SCP server enable, 333
SSH Secure Telnet client, 338
SSH Secure Telnet client configuration (password authentication-enabled), 362
SSH Secure Telnet client configuration (publickey authentication-enabled), 365
SSH Secure Telnet configuration, 353
SSH Secure Telnet configuration (128-bit Suite B), 367
SSH Secure Telnet server configuration (password authentication-enabled), 354
SSH Secure Telnet server configuration (publickey authentication-enabled), 356
SSH Secure Telnet server connection establishment, 339
SSH Secure Telnet server enable, 332
SSH server configuration, 331
SSH SFTP client, 342
SSH SFTP client configuration (publickey authentication-enabled), 374
SSH SFTP configuration, 371
SSH SFTP configuration (192-bit Suite B), 377
SSH SFTP server configuration (password authentication-enabled), 372
SSH SFTP server enable, 333
SSL server policy configuration, 394
uRPF configuration, 442

DF bit
security IPsec packet DF bit clear, 276
security IPsec packet DF bit copy, 276
security IPsec packet DF bit set, 276

DH
IPsec IKEv2 DH guessing, 310

DH algorithm
security IPsec IKE, 292
security IPsec PFS, 292

DHCP
802.1X EAD assistant, 100
dynamic IPv4 source guard (IPv4SG)+DHCP relay agent configuration, 407
dynamic IPv4 source guard (IPv4SG)+DHCP snooping configuration, 406
dynamic IPv6 source guard (IPv6SG)+DHCPv6 snooping configuration, 409
security portal authentication extended re-DHCP, 162
security portal authentication modes, 126
security portal authentication process, 127
security portal authentication re-DHCP, 153
security portal authentication re-DHCP process (with CHAP/PAP authentication), 128
troubleshooting security portal authentication users cannot log in (re-DHCP), 184
digital certificate
PKI CA certificate, 226
PKI CA policy, 227
PKI certificate export, 237
PKI certificate import/export, 248
PKI certificate obtain, 234
PKI certificate removal, 237
PKI certificate request, 232
PKI certificate request (automatic), 233
PKI certificate request (manual), 233
PKI certificate request abort, 234
PKI certificate verification, 235
PKI certificate-based access control policy, 238
PKI configuration, 226, 229, 239
PKI CRL, 226
PKI domain configuration, 230
PKI entity configuration, 229
PKI local certificate, 226
PKI OpenCA server certificate request, 245
PKI peer certificate, 226
PKI RA certificate, 226
PKI RSA Keon CA server certificate request, 239
PKI storage path, 236
PKI verification (CRL checking), 235
PKI verification (w/o CRL checking), 236
PKI Windows 2003 CA server certificate request, 242
Digital Signature Algorithm. Use DSA
direct portal authentication mode, 126, 127
directory
AAA LDAP directory service, 9
SSH SFTP, 347
displaying
802.1X, 93
AAA, 49
AAA HWTACACS, 39
AAA LDAP, 42
AAA local users/user groups, 22
AAA RADIUS, 33
ARP attack detection, 423
ARP attack detection (source MAC-based), 415
ARP attack protection (unresolvable IP attack), 412
crypto engine, 443
FIPS, 449
host public key, 219
IP source guard (IPSG), 405
IPsec IKEv2, 318
IPv4 source guard (IPv4SG), 405
IPv6 ND attack defense RA guard, 482
IPv6 ND attack detection, 479
IPv6 source guard (IPv6SG), 405
MAC authentication, 115
MACsec, 469
MFF, 434
PKI, 239
port security, 195
public key, 221
security IPsec, 280
security IPsec IKE, 301
security password control, 213
security portal authentication, 145
security user profile, 455
SSH, 353
SSH SFTP help information, 347
SSL, 399
uRPF, 441
distributing
local host public key, 219
domain
802.1X mandatory port authentication domain, 86
802.1X supported domain name delimiters, 92
AAA ISP domain accounting method, 47
AAA ISP domain attribute, 44
AAA ISP domain authentication method, 44
AAA ISP domain authorization method, 45
MAC authentication, 108
PKI domain configuration, 230
security portal authentication domain, 135
Don't Fragment bit. See DF bit
DPD
IPsec IKEv2 DPD, 317
security IPsec IKE DPD, 298
DSA
host public key display, 219
host public key export, 219
peer host public key entry, 221
public key import from file, 223
public key management, 217, 221
security IPsec IKE signature authentication, 291
SSH client host public key configuration, 334
SSH Secure Telnet client configuration (publickey authentication-enabled), 365
dst-mac validity check (ARP attack detection), 421
dynamic
IP source guard (IPSG) dynamic binding, 401
IPv4 source guard (IPv4SG)+DHCP relay agent configuration, 407
IPv4 source guard (IPv4SG)+DHCP snooping configuration, 406
IPv6 source guard (IPv6SG)+DHCPv6 snooping configuration, 409

E
EAD
802.1X authentication+EAD assistant, 79
802.1X EAD assistant, 93, 100
troubleshooting 802.1X EAD assistant Web browser users, 102
EAP
802.1X EAP over RADIUS, 66
802.1X EAP relay enable, 81
802.1X EAP termination enable, 81
802.1X EAP termination mode authentication, 70
802.1X packet format, 65
802.1X RADIUS EAP-Message attribute, 66
802.1X RADIUS Message-Authentication attribute, 67
802.1X relay authentication, 69
802.1X relay/termination authentication, 68
EAPOL
802.1X authentication (access device initiated), 67
802.1X authentication (client-initiated), 67
802.1X packet format, 66
ECDSA
feature and software version compatibility, 331
peer host public key entry, 221
public key import from file, 223
public key management, 217, 221
Elliptic Curve Digital Signature Algorithm. Use ECDSA
email (PKI secure), 228
enabling
802.1X, 80
802.1X critical voice VLAN, 91
802.1X EAP relay, 81
802.1X EAP termination, 81
802.1X guest VLAN assignment delay, 88
802.1X periodic online user reauthentication, 87
AAA RADIUS server load sharing, 29
AAA RADIUS session-control, 48
AAA RADIUS SNMP notification, 32
ARP attack detection logging, 422
IPsec IKEv2 cookie challenge, 317
IPv4 source guard (IPv4SG) on interface, 402
IPv6 ND attack defense RA guard logging, 482
IPv6 source guard (IPv6SG) on interface, 403
MAC authentication, 107
MAC authentication critical voice VLAN, 113
MAC authentication multi-VLAN mode, 109
MAC authentication offline detection, 114
MACsec desire, 465
MACsec MKA, 465
MFF, 433
MFF periodic gateway probe, 434
NETCONF-over-SSH, 333
parallel processing with 802.1X authentication, 110
port security, 188
port security authorization-fail-offline, 194
port security MAC move, 193
port security SNMP notification, 195
security IPsec ACL de-encapsulated packet check, 273
security IPsec IKE invalid SPI recovery, 299
security IPsec packet logging, 276
security IPsec QoS pre-classify, 276
security password control, 209
security portal authentication, 131
security portal authentication roaming, 141

501
SSH SCP server, 333
SSH Secure Telnet server, 332
SSH SFTP server, 333
uRPF, 441

encapsulating
802.1X RADIUS EAP-Message attribute, 66
security IPsec ACL de-encapsulated packet check, 273
security IPsec anti-replay, 274
security IPsec configuration, 259, 280
security IPsec RIPvng, 285
security IPsec transport mode, 260
security IPsec tunnel for IPv4 packets (IKE-based), 283
security IPsec tunnel for IPv4 packets (manual), 280
security IPsec tunnel mode, 260

encrypting
crypto engine configuration, 443
MACsec data encryption, 461
public key management, 217, 221
security IPsec, 262
security IPsec configuration, 259, 280
security IPsec encryption algorithm (3DES), 262
security IPsec encryption algorithm (AES), 262
security IPsec encryption algorithm (DES), 262
security IPsec RIPvng, 285
security IPsec tunnel for IPv4 packets (IKE-based), 283
security IPsec tunnel for IPv4 packets (manual), 280
SSH configuration, 328
SSH server configuration, 331
SSL services, 393

entering
FIPS mode (automatic reboot), 445, 449
FIPS mode (manual reboot), 445, 450
peer host public key, 221, 221
SSH client host public key, 334

ESP
IPsec security protocol 50, 260

establishing
security IPsec tunnel establishment, 263
security SSH SCP server connection, 348
security SSH SCP server connection based on Suite B, 351
security SSH Secure Telnet server connection based on Suite B, 342
SSH Secure Telnet server connection, 339

SSH SFTP server connection, 343
SSH SFTP server connection based on Suite B, 346

Ethernet
802.1X overview, 64
ARP attack protection configuration, 411

exporting
host public key, 219
PKI certificate, 237
PKI certificate import/export, 248
troubleshooting PKI certificate export failure, 257

extending
security portal authentication extended cross-subnet, 166
security portal authentication extended direct, 159
security portal authentication extended re-DHCP, 162

F
fail-permit feature (portal), 139
feature and software version compatibility
ECDSA, 331
Suite B, 331

Federal Information Processing Standard. Use FIPS file
portal authentication file name rules, 143
SSH SCP file transfer+password authentication, 381
SSH SFTP, 347

filtering
ARP packet filtering configuration, 428, 429

FIPS
configuration, 444, 449
configuration restrictions, 444
display, 449
mode configuration, 445
mode entry, 445
mode entry (automatic reboot), 449
mode entry (manual reboot), 450
mode exit, 447
mode exit (automatic reboot), 452
mode exit (manual reboot), 452
mode system changes, 446
self-test, 447
self-test trigger, 449

FIPS compliance
AAA, 16
password control, 209
PKI, 229
public key, 217
security IPsec, 263
security IPsec IKE, 292
SSH, 331
SSL, 394
fixed ARP
configuration, 426
configuration restrictions, 426
forcing
security portal authentication forced type, 123
format
802.1X EAP packet format, 65
802.1X EAPOL packet format, 66
802.1X packet, 65
AAA HWTACACS username, 37
AAA RADIUS packet format, 3
AAA RADIUS username, 26
MAC authentication user account, 108
forwarding
about IPv6 ND attack defense, 477
ARP attack detection restricted forwarding, 422
ARP attack detection restricted forwarding configuration, 424
dynamic IPv4 source guard (IPv4SG)+DHCP relay agent configuration, 407
dynamic IPv4 source guard (IPv4SG)+DHCP snooping configuration, 406
dynamic IPv6 source guard (IPv6SG)+DHCPv6 snooping configuration, 409
IP source guard (IPSG) configuration, 400, 401, 405
IPv6 ND attack defense configuration, 477
IPv6 ND attack defense RA guard configuration, 481, 483
IPv6 ND attack detection, 479
static IPv4 source guard (IPv4SG) configuration, 405
static IPv6 source guard (IPv6SG) configuration, 408
fragment
security IPsec packet DF bit, 276
TCP fragment attack prevention, 460
frame
port security configuration, 185, 188
FTP
AAA RADIUS Login-Service attribute check method, 32
local host public key distribution, 219
SSH SFTP client configuration (publickey authentication-enabled), 374
SSH SFTP client device, 342
SSH SFTP configuration, 371
SSH SFTP configuration (192-bit Suite B), 377
SSH SFTP directories, 347
SSH SFTP files, 347
SSH SFTP packet source IP address, 342
SSH SFTP server configuration (password authentication-enabled), 372
SSH SFTP server connection establishment, 343
SSH SFTP server connection establishment based on Suite B, 346
SSH SFTP server connection termination, 348
Fully Qualified Domain Name. Use FQDN function
security portal authentication extended functions, 123
G
gateway
ARP gateway protection, 427, 428
MFF periodic gateway probe, 434
generating
SSH server local key pair, 332
global
security IPsec IKE global identity information, 297
global parameter
IPsec IKEv2 global parameters, 317
group
MACsec group CAK, 461
guest VLAN
802.1X authentication, 74
802.1X configuration, 87, 96
MAC authentication, 104
MAC authentication configuration, 111
H
H3C
AAA RADIUS H3C proprietary attributes, 15
handshaking
802.1X online user handshake, 84
SSL handshake protocol, 393
hardware
crypto engine configuration, 443
history
security password history, 207
host
local host public key distribution, 219
peer host public key configuration, 220
peer host public key entry, 221, 221
peer host public key import from file, 220
public key display, 219
public key export, 219
SSH client host public key configuration, 334

HTTP
SSL configuration, 393, 394

HW Terminal Access Controller Access Control System. Use HWTACACS

HWTACACS
AAA configuration, 1, 17, 49
AAA for SSH user, 49
AAA implementation, 6
AAA local user configuration, 18
AAA MPLS L3VPN implementation, 13
AAA scheme, 18
accounting server, 35
authentication server, 34
authorization server, 34
display, 39
HWTACACS/RADIUS differences, 7
maintain, 39
outgoing packet source IP address, 37
packet exchange process, 7
protocols and standards, 13
scheme configuration, 33
scheme creation, 34
scheme VPN, 36
shared keys, 36
SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
timer set), 38
traffic statistics units, 37
troubleshooting, 62
username format, 37

Hypertext Transfer Protocol. Use HTTP

I
identity
security IPsec IKE global identity information, 297

ignoring
port security server authorization information, 193

IKE, 290, See also ISAKMP
configuration, 290, 292, 301
configuration (main mode/pre-shared key authentication), 301
DH algorithm, 292
displaying, 301
DPD configuration, 298
FIPS compliance, 292
global identity information, 297

identity authentication, 291
invalid SPI recovery, 299
IPsec negotiation mode, 261
IPsec policy (IKE-based), 269
IPsec policy (IKE-based/direct), 270
IPsec policy (IKE-based/template), 271
IPsec SA, 261
IPsec tunnel establishment, 263
IPsec tunnel for IPv4 packets (IKE-based), 283
keepalive, 298
keychain configuration, 296
maintaining, 301
NAT keepalive, 298
negotiation, 290
PFS, 292
profile configuration, 293
proposal configuration, 295
protocols and standards, 292
SA max number set, 300
security mechanism, 291
SNMP notification, 300
troubleshooting, 304
troubleshooting negotiation failure (no proposal match), 304
troubleshooting negotiation failure (no proposal or keychain specified correctly), 304

IKEv2, 309, See also ISAKMP
configuration, 309, 311, 318
cookie challenge, 310, 317
DH guessing, 310
display, 318
DPD configuration, 317
global parameter configuration, 317
keychain configuration, 316
maintain, 318
message retransmission, 310
NAT keepalive, 317
negotiation, 309
policy configuration, 314
pre-shared key authentication, 318
profile configuration, 311
proposal configuration, 314
protocols and standards, 310
RSA signature authentication, 321
SA rekeying, 310
troubleshoot, 326
troubleshoot negotiation failure (no proposal match), 326

IMC
AAA RADIUS session-control, 48
implementing
802.1X MAC-based access control, 72
802.1X port-based access control, 72
AAA for MPLS L3VPNs, 13
AAA HWTACACS, 6
AAA LDAP, 9
AAA on device, 11
AAA RADIUS, 2
security ACL-based IPsec, 262, 264
security application-based IPsec, 263
security IPsec, 262
importing
peer host public key from file, 220
PKI certificate import/export, 248
public key from file, 223
SSH client host public key, 335
troubleshooting PKI CA certificate import failure, 256
troubleshooting PKI local certificate import failure, 257
initiating
802.1X authentication, 67, 68
interface
security portal authentication Web server reference, 132
Internet
SSL configuration, 393, 394
Internet Key Exchange. Use IKE
intrusion detection/protection
port security blockmac mode, 191
port security disableport mode, 191
port security disableport-temporarily mode, 191
port security feature, 185
IP
security. Use IPsec
uRPF configuration, 442
uRPF enable, 441
IP addressing
AAA HWTACACS outgoing packet source IP address, 37
AAA LDAP server IP address, 40
AAA RADIUS outgoing packet source IP address, 29
AAA RADIUS security policy server IP address, 32
ARP attack detection configuration (user+packet validity check), 423
ARP attack detection ip validity check, 421
ARP attack detection restricted forwarding configuration, 424
ARP attack protection (unresolvable IP attack), 411, 413
ARP attack protection configuration, 411
ARP filtering configuration, 429
ARP gateway protection, 428
authorized ARP configuration (DHCP relay agent), 419
authorized ARP configuration (DHCP server), 418
MFF server IP address, 434
SSH Secure Telnet packet source IP address, 338
SSH SFTP packet source IP address, 342
uRPF configuration, 438
IP source guard
IPv4. See IPv4 source guard
IPv6. See IPv6 source guard
IP source guard (IPSG)
configuration, 400, 401, 405
display, 405
dynamic binding, 401
maintain, 405
static binding, 400
IPoE
security user profile configuration, 454
IPsec
ACL configuration, 265
ACL de-encapsulated packet check, 273
ACL IPsec anti-replay, 274
ACL rule keywords, 265
ACL-based implementation, 264
ACL-based IPsec, 262
application-based IPsec, 263
authentication, 262
authentication algorithms, 262
configuration, 259, 280
configuration restrictions, 267
displaying, 280
encapsulation modes, 260
encryption, 262
encryption algorithms, 262
FIPS compliance, 263
IKE (main mode/pre-shared key authentication), 301
IKE configuration, 290, 292, 301
IKE DPD, 298
IKE global identity information, 297
IKE identity authentication, 291
IKE invalid SPI recovery, 299
IKE keepalive, 298
IKE keychain, 296
IKE NAT keepalive, 298
IKE negotiation, 290
IKE negotiation mode, 261
IKE profile configuration, 293
IKE proposal, 295
IKE SA max number, 300
IKE security mechanism, 291
IKE SNMP notification, 300
IKEv2 configuration, 309, 311, 318
IKEv2 cookie challenge, 317
IKEv2 DPD configuration, 317
IKEv2 global parameters, 317
IKEv2 keychain, 316
IKEv2 NAT keepalive, 317
IKEv2 negotiation, 309
IKEv2 policy configuration, 314
IKEv2 profile configuration, 311
IKEv2 proposal configuration, 314
IKEv2+pre-shared key authentication, 318
IKEv2+RSA signature authentication, 321
implementation, 262
IPSec anti-replay window and sequence number synchronization, 274
IPv6. See IPv6 IPsec maintaining, 280
mirror image ACLs, 265
non-mirror image ACLs, 265
packet DF bit, 276
packet logging enable, 276
PKI configuration, 226, 229, 239
policy (IKE-based/direct), 270
policy application to interface, 273
policy configuration, 267
policy configuration (IKE-based), 269
policy configuration (IKE-based/template), 271
policy configuration restrictions, 269
protocols and standards, 263
QoS pre-classify enable, 276
RIPvng configuration, 285
SA, 261
security protocols, 260
SNMP notification configuration, 279
source interface policy bind, 275
transform set, 265
troubleshoot IKEv2, 326
troubleshoot IKEv2 negotiation failure (no proposal match), 326
troubleshoot SA negotiation failure (no transform set match), 326
troubleshoot SA negotiation failure (tunnel failure), 326
troubleshooting IKE, 304
troubleshooting IKE negotiation failure (no proposal match), 304
troubleshooting IKE negotiation failure (no proposal or keychain specified correctly), 304
troubleshooting SA negotiation failure (invalid identity info), 305
troubleshooting SA negotiation failure (no transform set match), 305
tunnel establishment, 263
tunnel for IPv4 packets (IKE-based), 283
tunnel for IPv4 packets (manual), 280
IPv4
security IPsec tunnel for IPv4 packets (IKE-based), 283
security IPsec tunnel for IPv4 packets (manual), 280
source guard. See IPv4 source guard
SSH SCP client device, 348
SSH Secure Telnet server connection establishment, 339
SSH SFTP server connection establishment, 343
SSH SFTP server connection establishment based on Suite B, 346
IPv4 source guard (IPv4SG) configuration, 400, 401, 402, 405
display, 405
dynamic configuration+DHCP relay agent, 407
dynamic configuration+DHCP snooping, 406
enable on interface, 402
maintain, 405
static binding configuration, 402
static configuration, 405
IPv6
IPsec. See IPv6 IPsec
ND attack defense. See IPv6 ND attack defense
source guard. See IPv6 source guard
SSH SCP client device, 348
SSH Secure Telnet server connection establishment, 339
SSH SFTP server connection establishment, 343
SSH SFTP server connection establishment based on Suite B, 346
IPv6 IPsec
routing protocol profile, 278
routing protocols configuration, 277
IPv6 ND attack defense
about ND attack detection, 478
about RA guard, 481
configuration, 477
configuring ND attack detection, 478
device role, 481
RA guard configuration, 481, 483
user attribute, 41
versions, 40
Lightweight Directory Access Protocol. Use LDAP
limiting
ARP packet rate limit, 413
port security secure MAC addresses, 189
load sharing
AAA RADIUS server load sharing, 29
local
802.1X authorization VLAN, 72
AAA local accounting method, 12
AAA local authentication, 12
AAA local authentication configuration, 17
AAA local authorization method, 12
AAA local user, 18
AAA SSH user local authentication+HWTACACS
authorization+RADIUS accounting, 50
host public key distribution, 219
key pair creation, 217
key pair destruction, 220
MAC authentication (local), 115
MAC authentication method, 103
PKI digital certificate, 226
portal authentication local portal Web server, 125, 142
portal authentication local portal Web server configuration, 144
portal authentication local portal Web server+client interaction protocols, 125
security password control local user parameters, 212
troubleshooting PKI certificate obtain failure, 254
troubleshooting PKI certificate request failure, 255
troubleshooting PKI local certificate import failure, 257
local 802.1X authentication
QoS, 455
user profile configuration, 455
local 802.1X authentication configuration
QoS, 455
local 802.1X authorization
QoS, 455
user profile configuration, 455
local 802.1X authorization configuration
QoS, 455
logging
ARP attack detection logging enable, 422
security IPsec packet logging enable, 276
security password events, 208
logging in
AAA concurrent login user max, 48
RADIUS Login-Service attribute, 32
logging out
security portal authentication users, 142
login
security password expired login, 207
security password user first login, 208
security password user login attempt limit, 208
security password user login control, 208
M
MAC
802.1X MAC-based access control, 72
address. See MAC addressing
authentication. See MAC authentication
security. Use MACsec
SSL services, 393
MAC address
802.1X authentication (client-initiated), 67
MAC addressing
802.1X authentication (access device initiated), 67
ARP attack detection (source MAC-based), 414, 415
ARP attack protection configuration, 411
ARP packet source MAC consistency check, 416
dynamic IPv4 source guard (IPv4SG)+DHCP
relay agent configuration, 407
dynamic IPv4 source guard (IPv4SG)+DHCP
snooping configuration, 406
dynamic IPv6 source guard (IPv6SG)+DHCPv6
snooping configuration, 409
IP source guard (IPSG) configuration, 400, 401, 405
MAC authentication, 107, 115
MAC authentication (local), 115
MAC authentication (RADIUS-based), 117
MAC authentication configuration, 103
MFF configuration, 431, 433, 435
MFF configuration (manual-mode in ring network), 436
MFF configuration (manual-mode in tree network), 435
port security client
macAddressElseUserLoginSecure, 201
port security MAC address autoLearn, 196
port security macAddressWithRadius, 187
port security secure MAC address, 191
port security secure MAC address port limit, 189
static IPv4 source guard (IPv4SG) configuration, 405
static IPv6 source guard (IPv6SG) configuration, 408
troubleshooting port security secure MAC addresses, 205
MAC authentication
ACL assignment, 105, 119
authorization VLAN, 104
current port users max, 109
critical VLAN, 105
critical VLAN configuration, 112
critical voice VLAN enable, 113
delay configuration, 110
display, 115
domain specification, 108
enable, 107
guest VLAN, 104
guest VLAN configuration, 111
keep-online, 114
local authentication, 115
maintain, 115
methods, 103
multi-VLAN mode configuration, 109
offline detection enable, 114
parallel processing with 802.1X authentication, 110
periodic reauthentication, 106
port security authentication control mode, 185
port security client
macAddressElseUserLoginSecure, 201
port security client userLoginWithOUI, 198
port security configuration, 185, 188, 196
port security features, 190
port security intrusion protection, 191
port security MAC address autoLearn, 196
port security MAC move, 193
port security MAC+802.1X authentication, 187
port security mode, 189
port security NTK, 190
RADIUS-based, 117
timer configuration, 108
user account format, 108
user account policies, 103
user profile assignment, 106
VLAN assignment, 104
MAC learning
port security autoLearn MAC learning control, 186
port security MAC learning control modes, 185
port security secure MAC learning control, 186
MAC-forced forwarding. Use MFF
MACsec
application mode, 462
basic concepts, 461
client-oriented configuration, 470
confidentiality offset configuration, 467
desire enable, 465
device-oriented configuration, 473
display, 469
maintain, 469
MKA enable, 465
MKA key server priority configuration, 466
operation (client-oriented), 462
operation (device-oriented), 462
preshared key configuration, 466
protection parameter configuration (interface view), 467
protection parameter configuration (MKA policy), 468
protocols and standards, 464
replay protection configuration, 468
services, 461
troubleshoot, 476
validation mode configuration, 468
maintaining
802.1X, 93
AAA HWTACACS, 39
AAA RADIUS, 33
ARP attack detection, 423
crypto engine, 443
IP source guard (IPSG), 405
IPsec IKEv2, 318
IPv4 source guard (IPv4SG), 405
IPv6 ND attack defense RA guard, 482
IPv6 ND attack detection, 479
IPv6 source guard (IPv6SG), 405
MAC authentication, 115
MACsec, 469
security IPsec, 280
security IPsec IKE, 301
security password control, 213
security portal authentication, 145
managing
public key, 217, 221
manual
FIPS mode (manual reboot), 445
FIPS mode entry (manual reboot), 450
FIPS mode exit (manual reboot), 447, 452
MFF operation mode, 432
Media Access Control Security. Use MACsec message
ARP attack protection configuration, 411
IPsec IKEv2 message retransmission, 310
Message Authentication Code. Use MAC

MFF
- basic concepts, 432
- configuration, 431, 433, 435
  configuration (manual-mode in ring network), 436
  configuration (manual-mode in tree network), 435
- display, 434
- enable, 433
- how it works, 433
- network port, 432
- network port configuration, 433
- operation modes, 432
- periodic gateway probe enable, 434
- protocols and standards, 433
- server IP address, 434
- user port, 432

minimum password length, 206

mirroring
- security IPsec mirror image ACLs, 265
- security IPsec non-mirror image ACLs, 265

MKA
- MACsec enable, 465
- MACsec MKA key server priority, 466
- policy application, 469
- policy configuration, 468

mode
- 802.1X EAP relay/termination comparison, 68
- 802.1X multicast trigger, 67, 85
- 802.1X unicast trigger, 67, 85
- FIPS, 445
- MAC authentication multi-VLAN, 109
- MACsec application (client-oriented), 462
- MACsec application (device-oriented), 462
- MACsec validation, 468
- MFF manual operation, 432
- PKI offline, 232
- PKI online, 232
- port security, 189
- port security authentication control, 185
- port security autoLearn MAC learning control, 186
- port security MAC learning control, 185
- port security MAC learning control autoLearn, 185
- port security MAC learning control secure, 185
- port security macAddressWithRadius authentication, 187
- port security secure MAC learning control, 186
- port security userLogin 802.1X authentication, 187
- port security userLoginSecure 802.1X authentication, 187
- port security userLoginSecureExt 802.1X authentication, 187
- port security userLoginWithOUI 802.1X authentication, 187
- security IPsec ACL-based implementation aggregation, 262
- security IPsec ACL-based implementation per-host, 262
- security IPsec ACL-based implementation standard, 262
- security IPsec application-based implementation, 263
- security IPsec encapsulation transport, 260
- security IPsec encapsulation tunnel, 260
- security IPsec IKE negotiation, 261
- security IPsec IKE negotiation (time-based lifetime), 261
- security IPsec IKE negotiation (traffic-based lifetime), 261
- troubleshooting port security mode cannot be set, 204
- uRPF loose check, 438
- uRPF strict check, 438

MPLS L3VPN
- AAA implementation, 13
- PKI support, 228
- security portal authentication (cross-subnet for MPLS L3VPN), 177

multicast
- 802.1X multicast trigger mode, 67, 85

N

NAS
- AAA configuration, 17
- AAA device implementation, 11
- AAA HWTACACS implementation, 6
- AAA LDAP implementation, 9
- AAA MPLS L3VPN implementation, 13
- AAA NAS-ID profile configuration, 48
- AAA RADIUS implementation, 2
- AAA RADIUS security policy server IP address, 32
- applying interface NAS-ID profile (RADIUS), 141
- port security NAS-ID profile, 194
NAT
IPsec IKEv2 keepalive, 317
security IPsec IKE keepalive, 298
ND attack defense
IPv6. See IPv6 ND attack defense
need to know. Use NTK
negotiating
IPsec IKEv2 negotiation, 309
security IPsec IKE negotiation, 290
security IPsec IKE negotiation mode, 261

NETCONF
enable over SSH, 333
Secure Telnet client user line configuration, 334
SSH, 328
SSH client user line configuration, 334
SSH+password authentication configuration, 390

network
802.1X access control method, 82
802.1X architecture, 64
802.1X authentication, 67, 68
802.1X authentication attempts max number for MAC authenticated users, 83
802.1X authentication request attempts max, 83
802.1X authentication server timeout timer, 83
802.1X authentication trigger, 85
802.1X Auth-Fail VLAN, 75, 89
802.1X authorization state, 82
802.1X authorization VLAN configuration, 96
802.1X basic configuration, 94
802.1X concurrent port users max, 82
802.1X critical VLAN, 76, 90, 91
802.1X critical voice VLAN, 78, 91
802.1X EAD assistant, 93
802.1X EAP over RADIUS, 66
802.1X EAP relay authentication, 69
802.1X EAP relay enable, 81
802.1X EAP relay/termination, 68
802.1X EAP termination enable, 81
802.1X EAP termination mode authentication, 70
802.1X EAP-Success packets sending, 91
802.1X guest VLAN, 74, 87
802.1X guest VLAN assignment delay, 88
802.1X guest VLAN configuration, 96
802.1X online user handshake, 84
802.1X packet format, 65
802.1X periodic online user reauthentication, 87
802.1X related protocols, 65
802.1X VLAN manipulation, 72
802.1X+ACL assignment configuration, 98
AAA device implementation, 11
AAA HWTACACS implementation, 6
AAA HWTACACS scheme, 33
AAA HWTACACS server SSH user, 49
AAA ISP domain accounting method, 47
AAA ISP domain attribute, 44
AAA ISP domain authentication method, 44
AAA ISP domain authorization method, 45
AAA ISP domain creation, 43
AAA ISP domain method, 43
AAA LDAP implementation, 9
AAA LDAP scheme, 40
AAA LDAP server SSH user authentication, 56
AAA local user, 18
AAA MPLS L3VPN implementation, 13
AAA NAS-ID profile configuration, 48
AAA network access user, 18
AAA RADIUS implementation, 2
AAA RADIUS scheme, 22
AAA RADIUS server SSH user authentication+authorization, 52
AAA scheme, 18
AAA SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
applying interface NAS-ID profile, 141
ARP active acknowledgement, 417
ARP attack detection (source MAC-based), 414, 415
ARP attack detection configuration, 420
ARP attack detection configuration (user+packet validity check), 423
ARP attack detection logging enable, 422
ARP attack detection packet validity check, 421
ARP attack detection restricted forwarding, 422
ARP attack detection restricted forwarding configuration, 424
ARP attack detection user validity check, 420
ARP attack protection (unresolvable IP attack), 411, 413
ARP attack protection blackhole routing (unresolvable IP attack), 412
ARP attack protection source suppression (unresolvable IP attack), 412
ARP filtering configuration, 428, 429
ARP gateway protection, 427, 428
ARP packet rate limit, 413
ARP packet source MAC consistency check, 416
ARP scanning, 426
authorized ARP configuration, 417
authorized ARP configuration (DHCP relay agent), 419
authorized ARP configuration (DHCP server), 418
dynamic IPv4 source guard (IPv4SG)+DHCP relay agent configuration, 407
dynamic IPv4 source guard (IPv4SG)+DHCP snooping configuration, 406
dynamic IPv6 source guard (IPv6SG)+DHCPv6 snooping configuration, 409
FIPS mode entry (automatic reboot), 449
FIPS mode entry (manual reboot), 450
FIPS mode exit (automatic reboot), 452
FIPS mode exit (manual reboot), 452
fixed ARP configuration, 426
IP source guard (IPSG) dynamic binding, 401
IP source guard (IPSG) static binding, 400
IPsec IKEv2+pre-shared key authentication, 318
IPsec IKEv2+RSA signature authentication, 321
IPv4 source guard (IPv4SG) configuration, 402
IPv4 source guard (IPv4SG) enable on interface, 402
IPv4 source guard (IPv4SG) static binding configuration, 402
IPv6 ND attack defense device role, 481
IPv6 ND attack defense RA guard configuration, 481, 483
IPv6 ND attack defense RA guard logging enable, 482
IPv6 ND attack defense RA guard policy, 481
IPv6 ND attack detection, 478
IPv6 source guard (IPv6SG) configuration, 403
IPv6 source guard (IPv6SG) enable on interface, 403
IPv6 source guard (IPv6SG) static binding configuration, 404
MAC authentication (local), 115
MAC authentication (RADIUS-based), 117
MAC authentication ACL assignment, 105, 119
MAC authentication authorization VLAN, 104
MAC authentication concurrent port users max, 109
MAC authentication critical VLAN, 105, 112
MAC authentication critical voice VLAN, 113
MAC authentication delay, 110
MAC authentication domain, 108
MAC authentication guest VLAN, 104, 111
MAC authentication keep-online, 114
MAC authentication multi-VLAN mode, 109
MAC authentication offline detection enable, 114
MAC authentication timer, 108
MAC authentication user account format, 108
MAC authentication user profile assignment, 106
MAC authentication VLAN assignment, 104
MACsec application mode, 462
MACsec configuration (client-oriented), 470
MACsec configuration (device-oriented), 473
MACsec desire enable, 465
MACsec MKA enable, 465
MACsec preshared key, 466
MACsec protection parameter (interface view), 467
MACsec protection parameter (MKA policy), 468
MACsec services, 461
MFF configuration, 433
MFF configuration (manual-mode in ring network), 436
MFF configuration (manual-mode in tree network), 435
MFF network port, 432, 433
MFF periodic gateway probe, 434
NETCONF-over-SSH client user line, 334
NETCONF-over-SSH enable, 333
NETCONF-over-SSH+password authentication configuration, 390
parallel processing with 802.1X authentication, 110
peer host public key entry, 221
periodic MAC reauthentication, 106
PKI applications, 228
PKI architecture, 227
PKI CA policy, 227
PKI certificate import/export, 248
PKI certificate request, 232
PKI CRL, 226
PKI digital certificate, 226
PKI domain configuration, 230
PKI entity configuration, 229
PKI MPLS L3VPN support, 228
PKI OpenCA server certificate request, 245
PKI operation, 227
PKI RSA Keon CA server certificate request, 239
PKI storage path, 236
PKI Windows 2003 CA server certificate request, 242
port security authorization-fail-offline, 194
port security client
macAddressElseUserLoginSecure, 201
port security client userLoginWithOUI, 198
port security features, 185, 190
port security intrusion protection, 191
port security MAC address autoLearn, 196
port security MAC address learning control, 186
port security mode, 185, 189
port security NAS-ID profile, 194
port security NTK, 190
port security secure MAC address, 191
port security secure MAC address port limit, 189
port security SNMP notification, 195
portal authentication local portal Web server, 125, 142
portal authentication local portal Web server configuration, 144
public key import from file, 223
Secure Telnet client user line, 334
security IPsec ACL, 265
security IPsec ACL de-encapsulated packet check, 273
security IPsec ACL-based implementation, 262, 264
security IPsec anti-replay, 274
security IPsec anti-replay window and sequence number synchronization, 274
security IPsec application-based implementation, 263
security IPsec IKE SNMP notification, 300
security IPsec implementation, 262
security IPsec IPv6 routing protocol profile, 278
security IPsec IPv6 routing protocols, 277
security IPsec packet DF bit, 276
security IPsec packet logging enable, 276
security IPsec policy, 267
security IPsec policy (IKE-based), 269
security IPsec policy (IKE-based/direct), 270
security IPsec policy (IKE-based/template), 271
security IPsec policy application to interface, 273
security IPsec QoS pre-classify enable, 276
security IPsec SNMP notification, 279
security IPsec source interface policy bind, 275
security IPsec transform set, 265
security IPsec tunnel establishment, 263
security password control global parameters, 210
security password control local user parameters, 212
security password control user group parameters, 211
security portal authentication AAA server, 124
security portal authentication client, 124
security portal authentication domain, 135
security portal authentication system components, 123
security SSH SCP server connection establishment, 348
security SSH SCP server connection establishment based on Suite B, 351
security SSH Secure Telnet server connection establishment based on Suite B, 342
security super password control parameters, 212
SSH client host public key configuration, 334
SSH management parameters, 336
SSH SCP client device, 348
SSH SCP file transfer+password authentication, 381
SSH SCP server enable, 333
SSH Secure Telnet client configuration (password authentication-enabled), 362
SSH Secure Telnet client configuration (publickey authentication-enabled), 365
SSH Secure Telnet client device, 338
SSH Secure Telnet configuration, 353
SSH Secure Telnet configuration (128-bit Suite B), 367
SSH Secure Telnet packet source IP address, 338
SSH Secure Telnet server configuration (password authentication-enabled), 354
SSH Secure Telnet server configuration (publickey authentication-enabled), 356
SSH Secure Telnet server connection establishment, 339
SSH Secure Telnet server enable, 332
SSH server configuration, 331
SSH SFTP client configuration (publickey authentication-enabled), 374
SSH SFTP client device, 342
SSH SFTP configuration, 371
SSH SFTP configuration (192-bit Suite B), 377
SSH SFTP directories, 347
SSH SFTP files, 347
SSH SFTP packet source IP address, 342
SSH SFTP server configuration (password authentication-enabled), 372
SSH SFTP server connection establishment, 343
| SSH SFTP server connection establishment based on Suite B | 346 |
| SSH SFTP server connection termination | 348 |
| SSH SFTP server enable | 333 |
| SSH user configuration | 335 |
| SSH2 algorithms | 351 |
| SSH2 algorithms (encryption) | 352 |
| SSH2 algorithms (key exchange) | 352 |
| SSH2 algorithms (MAC) | 353 |
| SSH2 algorithms (public key) | 352 |
| SSL client policy configuration | 397 |
| SSL protocol stack | 393 |
| SSL server policy configuration | 394 |
| static IPv4 source guard (IPv4SG) configuration | 405 |
| static IPv6 source guard (IPv6SG) configuration | 408 |
| uRPF application | 441 |
| uRPF check modes | 438 |
| uRPF enable | 441 |
| uRPF operation | 438 |
| network management |  |
| 802.1X authentication configuration | 94 |
| 802.1X configuration | 72, 80 |
| 802.1X EAD assistant | 100 |
| 802.1X overview | 64 |
| AAA configuration | 1, 17, 49 |
| AAA HWTACACS/RADIUS differences | 7 |
| about IPv6 ND attack defense | 477 |
| ARP attack protection configuration | 411 |
| attack D&P configuration | 460 |
| crypto engine configuration | 443 |
| FIPS configuration | 444, 449 |
| IP source guard (IPSG) configuration | 400, 401, 405 |
| IPSec IKEv2 configuration | 309, 311, 318 |
| IPv6 ND attack defense configuration | 477 |
| IPv6 ND attack detection | 479 |
| MAC authentication | 107, 115 |
| MAC authentication configuration | 103 |
| MACsec configuration | 461, 465, 470 |
| MFF configuration | 431, 435 |
| PKI configuration | 226, 229, 239 |
| port security configuration | 185, 188, 196 |
| public key management | 217, 221 |
| security IPsec configuration | 259, 280 |
| security IPsec IKE (main mode/pre-shared key authentication) | 301 |
| security IPsec IKE configuration | 290, 292, 301 |
| security IPsec RIPng | 285 |
| security IPsec tunnel for IPv4 packets (IKE-based) | 283 |
| security IPsec tunnel for IPv4 packets (manual) | 280 |
| security password control | 209, 213 |
| security password control configuration | 206 |
| security portal authentication | 129 |
| security portal authentication configuration | 123 |
| security SSH SCP configuration | 381 |
| security SSH SCP configuration (Suite B) | 383 |
| security user profile configuration | 454 |
| SSH configuration | 328 |
| SSL configuration | 393, 394 |
| SSL services | 393 |
| uRPF configuration | 438, 442 |
| no |  |
| AAA no accounting method | 12 |
| AAA no authentication | 12 |
| AAA no authorization | 12 |
| notifying |  |
| AAA RADIUS SNMP notification | 32 |
| port security SNMP notification | 195 |
| security IPsec IKE SNMP notification | 300 |
| security IPsec SNMP notification | 279 |
| NTK |  |
| ntkonly mode | 190 |
| ntk-withbroadcasts mode | 190 |
| ntk-withmulticasts mode | 190 |
| port security feature | 185 |
| numbering |  |
| security IPsec IKE SA max number set | 300 |
| O |  |
| obtaining |  |
| PKI certificate | 234 |
| offline |  |
| MAC authentication offline detect | 108 |
| MAC authentication offline detection enable | 114 |
| PKI offline mode | 232 |
| port security authorization-fail-offline feature | 194 |
| offsetting |  |
| MACsec confidentiality offset | 467 |
| online |  |
| 802.1X online user handshake | 84 |
| 802.1X periodic online user reauthentication | 87 |
| MAC authentication keep-online | 114 |
| PKI online mode | 232 |
| port security authentication user online detection | 136 |
| OpenCA |  |
| PKI CA server certificate request | 245 |

514
packet filtering

about IPv6 ND attack defense, 477
dynamic IPv4 source guard (IPv4SG)+DHCP relay agent configuration, 407
dynamic IPv4 source guard (IPv4SG)+DHCP snooping configuration, 406
dynamic IPv6 source guard (IPv6SG)+DHCPv6 snooping configuration, 409

IP source guard (IPSG) configuration, 400, 401, 405
IPv6 ND attack defense configuration, 477
IPv6 ND attack defense RA guard configuration, 481, 483
IPv6 ND attack detection, 479
static IPv4 source guard (IPv4SG) configuration, 405
static IPv6 source guard (IPv6SG) configuration, 408

page

portal authentication authenticated user redirection, 144
portal authentication page file compression+saving rules, 144
portal authentication page request rules, 143
portal authentication post request rules, 143
pairwise CAK (MACsec), 461
parameter

AAA RADIUS accounting server parameters, 25
configuring SSH management parameters, 336
MACsec protection parameter (interface view), 467
MACsec protection parameter (MKA policy), 468
security password control global parameters, 210
security password control local user parameters, 212
security password control user group parameters, 211
security super password control parameters, 212

password

SSH password authentication, 329
SSH password-publickey authentication, 329
SSH SCP file transfer+password authentication, 381
SSH Secure Telnet client configuration (password authentication-enabled), 362
SSH Secure Telnet server configuration (password authentication-enabled), 354
SSH SFTP server configuration (password authentication-enabled), 372

password control

configuration, 206, 209, 213
displaying, 213
enable, 209
event logging, 208
expired password login, 207
FIPS compliance, 209
global parameters, 210
local user parameters, 212
maintaining, 213
max user account idle time, 208
password complexity checking, 206
password composition checking, 206
password expiration, 207, 207
password history, 207
password min length, 206
password not displayed, 208
password setting, 206
password updating, 207, 207
super parameters, 212
user first login, 208
user group parameters, 211
user login attempt limit, 208
user login control, 208
path
troubleshooting PKI storage path set failure, 258
peer
host public key configuration, 220
host public key entry, 221, 221
host public key import from file, 220
PKI digital certificate, 226
security IPsec implementation, 262
security IPsec SA, 261
security IPsec source interface policy bind, 275
Perfect Forward Secrecy. See PFS
periodic gateway probe (MFF), 434
periodic MAC reauthentication, 106
PFS (IKE), 292
PKI
applications, 228
architecture, 227
CA digital certificate, 226
CA policy, 227
certificate export, 237
certificate import/export, 248
certificate obtain, 234
certificate removal, 237
certificate request, 232
certificate request (automatic), 233
certificate request (manual), 233
certificate request abort, 234
certificate verification, 235
certificate verification (CRL checking), 235
certificate verification (w/o CRL checking), 236
certificate-based access control policy, 238
configuration, 226, 229, 239
CRL, 226
display, 239
domain configuration, 230
entity configuration, 229
FIPS compliance, 229
local digital certificate, 226
MPLS L3VPN support, 228
OpenCA server certificate request, 245
operation, 227
peer digital certificate, 226
peer host public key entry, 221
public key import from file, 223
public key management, 217, 221
RA digital certificate, 226
RSA Keon CA server certificate request, 239
storage path, 236
terminology, 226
troubleshoot CA certificate import failure, 256
troubleshoot CA certificate obtain failure, 254
troubleshoot certificate export failure, 257
troubleshoot configuration, 253
troubleshoot CRL obtain failure, 255
troubleshoot local certificate import failure, 257
troubleshoot local certificate obtain failure, 254
troubleshoot local certificate request failure, 255
troubleshoot storage path set failure, 258
Windows 2003 CA server certificate request configuration, 242
policy
AAA RADIUS security policy server IP address, 32
IPsec IKEv2 configuration, 314
IPv6 ND attack defense RA guard logging enable, 482
IPv6 ND attack defense RA guard policy, 481
MAC authentication user account policies, 103
MACsec MKA policy application, 469
MACsec MKA policy configuration, 468
MACsec protection parameter (MKA policy), 468
PKI CA policy, 227
PKI certificate-based access control policy, 238
security IPsec, 267
security IPsec application to interface, 273
security IPsec policy (IKE-based), 269
security IPsec policy (IKE-based/direct), 270
security IPsec policy (IKE-based/template), 271
security IPsec QoS pre-classify enable, 276
security IPsec source interface policy bind, 275
security IPsec transform set, 265
security password control, 209, 213
security password control configuration, 206
security portal authentication extended functions, 123
security portal authentication policy server, 124
SSL client policy configuration, 397
SSL server policy configuration, 394

802.1X Auth-Fail VLAN, 89
802.1X critical VLAN, 90, 91
802.1X critical voice VLAN, 91
802.1X guest VLAN, 87
applying interface NAS-ID profile, 141
direct portal authentication configuration (local portal Web server), 144, 179
MAC authentication, 107, 115
MAC authentication (local), 115
MAC authentication (RADIUS-based), 117
MAC authentication concurrent port users max, 109
MAC authentication configuration, 103
MAC authentication critical VLAN, 112
MAC authentication critical voice VLAN, 113
MAC authentication delay, 110
MAC authentication guest VLAN, 111
MAC authentication multi-VLAN mode, 109
MACsec protection parameter (interface view), 467
MACsec protection parameter (MKA policy), 468
MFF network port, 432, 433
MFF user port, 432
security. See port security
security portal authentication, 129
security portal authentication configuration, 123, 145
security portal authentication cross-subnet, 156
security portal authentication direct, 145
security portal authentication extended cross-subnet, 166
security portal authentication extended direct, 159
security portal authentication extended re-DHCP, 162
security portal authentication re-DHCP, 153
security portal authentication server detection+user synchronization, 169
port security
802.1X access control method, 82
802.1X authentication, 187
802.1X authentication configuration, 94
802.1X authorization state, 82
802.1X authorization status, 64
802.1X authorization VLAN configuration, 96
802.1X basic configuration, 94
802.1X concurrent port users max, 82
802.1X configuration, 72, 80
802.1X controlled/uncontrolled port, 64
802.1X guest VLAN configuration, 96
802.1X mandatory port authentication domain, 86
802.1X overview, 64
802.1X+ACL assignment configuration, 98
authentication modes, 185
authorization-fail-offline, 194
client macAddressElseUserLoginSecure, 201
client userLoginWithOUI, 198
configuration, 185, 188, 196
display, 195
enable, 188
feature configuration, 190
features, 185
intrusion protection, 191
intrusion protection feature, 185
MAC address autoLearn, 196
MAC address learning control, 186
MAC authentication, 187
MAC move enable, 193
MAC+802.1X authentication, 187
mode set, 189
NAS-ID profile application, 194
NTK configuration, 190
NTK feature, 185
secure MAC address, 191
secure MAC address port limit, 189
server authorization information ignore, 193
SNMP notification enable, 195
troubleshoot, 204
troubleshoot mode cannot be set, 204
troubleshoot secure MAC addresses, 205
portal
safety user profile configuration, 454
portal authentication
AAA server, 124
access device, 124
authenticated user redirection, 144
authentication destination subnet, 134
authentication modes, 126
authentication process, 127
authentication server, 124
authentication source subnet, 133
BAS-IP, 140
client, 124
cross-subnet, 156
cross-subnet for MPLS L3VPN, 177
detection features, 136
direct configuration, 145
direct configuration (local portal Web server), 144, 179
direct/cross-subnet authentication process (with CHAP/PAP authentication), 127
displaying, 145
domain specification, 135
enabling, 131
extended cross-subnet, 166
extended direct, 159
extended functions, 123
extended re-DHCP, 162
fail-permit configuration, 139
file name rules, 143
local portal Web server, 125
local portal Web server configuration, 142, 144
local portal Web server page customization, 125
local portal Web server+client interaction protocols, 125
maintaining, 145
max number users, 135
page customization, 142
page file compression+saving rules, 144
page request rules, 143
portal-free rule, 132
post request rules, 143
re-DHCP, 153
roaming enable, 141
security policy server, 124
server configuration, 130
server detection, 137
server detection+user synchronization, 169
system component interaction, 125
system components, 123
troubleshooting, 182
troubleshooting cannot log out users (access device), 182
troubleshooting cannot log out users (RADIUS server), 183
troubleshooting no page pushed for users, 182
troubleshooting users logged out still exist on server, 183
types, 123
user access control, 132
user logout, 142
user online detection, 136
user synchronization configuration, 138
users cannot log in (re-DHCP), 184
Web server, 124
Web server configuration, 130
Web server detection configuration, 138
Web server reference, 132
power-up self-test, 448
PPPoE
  security user profile configuration, 454
  preshared key (PSK)
    MACsec configuration, 466
preventing
detection and prevention. See attack D&P
priority
  MACsec MKA key server priority, 466
procedure
  applying interface NAS-ID profile, 141
  applying MACsec MKA policy, 469
  applying port security NAS-ID profile, 194
  applying security IPsec policy to interface, 273
  authenticating with 802.1X EAP relay, 69
  authenticating with 802.1X EAP termination mode, 70
  binding security IPsec source interface to policy, 275
  configuring security portal authentication (cross-subnet for MPLS L3VPN), 177
  configuring 802.1X, 80
  configuring 802.1X authentication trigger, 85
  configuring 802.1X Auth-Fail VLAN, 89
  configuring 802.1X authorization VLAN, 96
  configuring 802.1X basics, 94
  configuring 802.1X critical VLAN, 90, 91
  configuring 802.1X EAD assistant, 93, 100
  configuring 802.1X guest VLAN, 87, 96
  configuring 802.1X online user handshake, 84
  configuring 802.1X+ACL assignment, 98
  configuring AAA, 17
  configuring AAA HWTACACS schemes, 33
  configuring AAA HWTACACS server SSH user, 49
  configuring AAA ISP domain accounting method, 47
  configuring AAA ISP domain attribute, 44
  configuring AAA ISP domain authentication method, 44
  configuring AAA ISP domain authorization method, 45
  configuring AAA ISP domain method, 43
  configuring AAA LDAP administrator attributes, 41
  configuring AAA LDAP scheme, 40
  configuring AAA LDAP server IP address, 40
  configuring AAA LDAP server SSH user authentication, 56
configuring AAA LDAP user attributes, 41
configuring AAA local user, 18
configuring AAA local user attributes, 19
configuring AAA NAS-ID profile, 48
configuring AAA RADIUS accounting-on, 31
configuring AAA RADIUS Login-Service attribute check method, 32
configuring AAA RADIUS scheme, 22
configuring AAA RADIUS security policy server IP address, 32
configuring AAA RADIUS server SSH user authentication+authorization, 52
configuring AAA RADIUS server status detection test profile, 23
configuring AAA scheme, 18
configuring AAA SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
configuring AAA user group attributes, 21
configuring and applying IPv6 ND attack defense RA guard policy, 481
configuring ARP active acknowledgement, 417
configuring ARP attack detection, 420
configuring ARP attack detection (source MAC-based), 414, 415
configuring ARP attack detection (user+packet validity check), 423
configuring ARP attack detection packet validity check, 421
configuring ARP attack detection restricted forwarding, 422, 424
configuring ARP attack detection user validity check, 420
configuring ARP attack protection, 411
configuring ARP attack protection (unresolvable IP attack), 411, 413
configuring ARP attack protection blackhole routing (unresolvable IP attack), 412
configuring ARP attack protection source suppression (unresolvable IP attack), 412
configuring ARP filtering, 428, 429
configuring ARP gateway protection, 427, 428
configuring ARP packet rate limit, 413
configuring ARP packet source MAC consistency check, 416
configuring ARP scanning, 426
configuring authorized ARP (DHCP relay agent), 419
configuring authorized ARP (DHCP server), 418
configuring authorized ARP configuration, 417
configuring direct portal authentication (local portal Web server), 144, 179
configuring dynamic IPv4 source guard (IPv4SG)+DHCP snooping, 406
configuring dynamic IPv6 source guard (IPv6SG)+DHCPv6 snooping, 409
configuring FIPS mode, 445
configuring fixed ARP, 426
configuring IP source guard (IPSG), 401
configuring IPsec IKEv2, 311
configuring IPsec IKEv2 DPD, 317
configuring IPsec IKEv2 global parameters, 317
configuring IPsec IKEv2 keychain, 316
configuring IPsec IKEv2 NAT keepalive, 317
configuring IPsec IKEv2 policy, 314
configuring IPsec IKEv2 profile, 311
configuring IPsec IKEv2 proposal, 314
configuring IPsec IKEv2+pre-shared key authentication, 318
configuring IPsec IKEv2+RSA signature authentication, 321
configuring IPv4 source guard (IPv4SG), 402
configuring IPv4 source guard (IPv4SG) static binding, 402
configuring IPv6 ND attack defense RA guard, 481, 483
configuring IPv6 ND attack detection, 478, 478, 479
configuring IPv6 source guard (IPv6SG), 403
configuring IPv6 source guard (IPv6SG) static binding, 404
configuring MAC authentication, 107
configuring MAC authentication (local), 115
configuring MAC authentication (RADIUS-based), 117
configuring MAC authentication ACL assignment, 119
configuring MAC authentication critical VLAN, 112
configuring MAC authentication delay, 110
configuring MAC authentication guest VLAN, 111
configuring MAC authentication keep-online, 114
configuring MAC authentication multi-VLAN mode, 109
configuring MAC authentication timer, 108
configuring MAC authentication user account format, 108
configuring MACsec, 465
configuring MACsec (client-oriented), 470
configuring MACsec (device-oriented), 473
configuring MACsec confidentiality offset, 467
configuring MACsec MKA key server priority, 466
configuring MACsec MKA policy, 468
configuring MACsec preshared key, 466
configuring MACsec protection parameters (interface view), 467
configuring MACsec protection parameters (MKA policy), 468
configuring MACsec replay protection, 468
configuring MACsec validation mode, 468
configuring MFF, 433
configuring MFF (manual-mode in ring network), 436
configuring MFF (manual-mode in tree network), 435
configuring MFF network port, 433
configuring ND attack defense, 477
configuring NETCONF-over-SSH client user line, 334
configuring NETCONF-over-SSH+password authentication, 390
configuring peer host public key, 220
configuring PKI, 229
configuring PKI certificate import/export, 248
configuring PKI certificate request (automatic), 233
configuring PKI certificate request (manual), 233
configuring PKI certificate request abort, 234
configuring PKI certificate-based access control policy, 238
configuring PKI domain, 230
configuring PKI entity, 229
configuring PKI OpenCA server certificate request, 245
configuring PKI RSA Keon CA server certificate request, 239
configuring PKI Windows 2003 CA server certificate request, 242
configuring port security, 188
configuring port security client macAddressElseUserLoginSecure, 201
configuring port security client userLoginWithOUI, 198
configuring port security features, 190
configuring port security intrusion protection, 191
configuring port security MAC address autoLearn, 196
configuring port security NTK, 190
configuring port security secure MAC addresses, 191
configuring portal authentication local portal Web server, 142, 144
configuring QoS or CAR parameters, 455
configuring relay agent IPv4 source guard (IPv4SG)+DHCP relay agent, 407
configuring Secure Telnet client user line, 334
configuring security IPsec, 280
configuring security IPsec ACL, 265
configuring security IPsec ACL anti-replay, 274
configuring security IPsec anti-replay window and sequence number synchronization, 274
configuring security IPsec IKE, 292, 301
configuring security IPsec IKE (main mode/pre-shared key authentication), 301
configuring security IPsec IKE DPD, 298
configuring security IPsec IKE global identity information, 297
configuring security IPsec IKE keepalive, 298
configuring security IPsec IKE keychain, 296
configuring security IPsec IKE NAT keepalive, 298
configuring security IPsec IKE profile, 293
configuring security IPsec IKE proposal, 295
configuring security IPsec IKE SA max number, 300
configuring security IPsec IKE SNMP notification, 300
configuring security IPsec IPv6 routing protocol profile, 278
configuring security IPsec IPv6 routing protocols, 277
configuring security IPsec packet DF bit, 276
configuring security IPsec policy, 267
configuring security IPsec policy (IKE-based), 269
configuring security IPsec policy (IKE-based/direct), 270
configuring security IPsec policy (IKE-based/template), 271
configuring security IPsec RIPng, 285
configuring security IPsec SNMP notification, 279
configuring security IPsec transform set, 265
configuring security IPsec tunnel for IPv4 packets (IKE-based), 283
configuring security IPsec tunnel for IPv4 packets (manual), 280
configuring security password control, 209, 213
configuring security portal authentication, 129, 145
configuring security portal authentication destination subnet, 134
configuring security portal authentication detection features, 136
configuring security portal authentication direct, 145
configuring security portal authentication extended direct, 159
configuring security portal authentication fail-permit, 139
configuring security portal authentication portal-free rule, 132
configuring security portal authentication server, 130
configuring security portal authentication server BAS-IP, 140
configuring security portal authentication server detection, 137
configuring security portal authentication source subnet, 133
configuring security portal authentication user online detection, 136
configuring security portal authentication user synchronization, 138
configuring security portal authentication Web server, 130
configuring security portal authentication Web server detection, 138
configuring security SSH SCP, 381
configuring security SSH SCP (Suite B), 383
configuring security user profile, 454
configuring SSH client host public key, 334
configuring SSH device as Secure Telnet client, 338
configuring SSH device as server, 331
configuring SSH device as SFTP client, 342
configuring SSH management parameters, 336
configuring SSH SCP client device, 348
configuring SSH SCP file transfer+password authentication, 381
configuring SSH Secure Telnet client (password authentication-enabled), 362
configuring SSH Secure Telnet client (publickey authentication-enabled), 365
configuring SSH Secure Telnet server (password authentication-enabled), 354
configuring SSH Secure Telnet server (publickey authentication-enabled), 356
configuring SSH SFTP client publickey authentication, 374
configuring SSH SFTP server (password authentication-enabled), 372
configuring SSH user, 335
configuring SSH2 algorithms (encryption), 352
configuring SSH2 algorithms (key exchange), 352
configuring SSH2 algorithms (MAC), 353
configuring SSH2 algorithms (public key), 352
configuring SSL, 394
configuring SSL client policy, 397
configuring SSL server policy, 394
configuring static IPv4 source guard (IPv4SG), 405
configuring static IPv6 source guard (IPv6SG), 408
configuring TCP fragment attack prevention, 460
configuring uRPF, 442
configuring user profile, 455
configuring user profile parameters, 455
controlling security portal authentication user access, 132
creating AAA HWTACACS scheme, 34
creating AAA ISP domain, 43
creating AAA LDAP scheme, 42
creating AAA LDAP server, 40
creating AAA RADIUS scheme, 23
creating local key pair, 217
creating user profile, 454
destroying local key pair, 220
displaying 802.1X, 93
displaying AAA, 49
displaying AAA HWTACACS, 39
displaying AAA LDAP, 42
displaying AAA local users/user groups, 22
displaying AAA RADIUS, 33
displaying ARP attack detection, 423
displaying ARP attack detection (source MAC-based), 415
displaying ARP attack protection (unresolvable IP attack), 412
displaying crypto engine, 443
displaying FIPS, 449
displaying host public key, 219
displaying IP source guard (IPSG), 405
displaying IPsec IKEv2, 318
displaying IPv4 source guard (IPv4SG), 405
displaying IPv6 ND attack defense RA guard, 482
displaying IPv6 ND attack detection, 479
displaying IPv6 source guard (IPv6SG), 405
displaying MAC authentication, 115
displaying MACsec, 469
displaying MFF, 434
displaying port security, 195
displaying public key, 221
displaying security IPsec, 280
displaying security IPsec IKE, 301
displaying security password control, 213
displaying security PKI, 239
displaying security portal authentication, 145
displaying security user profile, 455
displaying SSH, 353
displaying SSH SFTP help information, 347
displaying SSL, 399
displaying uRPF, 441
distributing local host public key, 219
enabling 802.1X, 80
enabling 802.1X critical voice VLAN, 91
enabling 802.1X EAP relay, 81
enabling 802.1X EAP termination, 81
enabling 802.1X guest VLAN assignment delay, 88
enabling 802.1X periodic online user reauthentication, 87
enabling AAA RADIUS server load sharing, 29
enabling AAA RADIUS session-control, 48
enabling AAA RADIUS SNMP notification, 32
enabling ARP attack detection logging, 422
enabling IPSec IKEv2 cookie challenge, 317
enabling IPv4 source guard (IPv4SG) on interface, 402
enabling IPv6 ND attack defense RA guard logging, 482
enabling IPv6 source guard (IPv6SG) on interface, 403
enabling MAC authentication, 107
enabling MAC authentication critical voice VLAN, 113
enabling MAC authentication offline detection, 114
enabling MACsec desire, 465
enabling MACsec MKA, 465
enabling MFF, 433
enabling MFF periodic gateway probe, 434
enabling NETCONF-over-SSH, 333
enabling parallel processing with 802.1X authentication, 110
enabling port security, 188
enabling port security authorization-fail-offline, 194
enabling port security MAC move, 193
enabling port security SNMP notification, 195
enabling security IPSec ACL de-encapsulated packet check, 273
enabling security IPSec IKE invalid SPI recovery, 299
enabling security IPSec packet logging, 276
enabling security IPSec QoS pre-classify, 276
enabling security password control, 209
enabling security portal authentication, 131
enabling security portal authentication roaming, 141
enabling SSH SCP server, 333
enabling SSH Secure Telnet server, 332
enabling SSH SFTP server, 333
enabling uRPF, 441
entering FIPS mode (automatic reboot), 445, 449
entering FIPS mode (manual reboot), 445, 450
entering peer host public key, 221, 221
entering SSH client host public key, 334
establishing security SSH SCP server connection, 348
establishing security SSH SCP server connection based on Suite B, 351
establishing security SSH Secure Telnet server connection based on Suite B, 342
establishing SSH Secure Telnet server connection, 339
establishing SSH SFTP server connection, 343
establishing SSH SFTP server connection based on Suite B, 346
exiting FIPS mode, 447
exiting FIPS mode (automatic reboot), 447, 452
exiting FIPS mode (manual reboot), 447, 452
exporting host public key, 219
exporting PKI certificate, 237
generating SSH server local key pair, 332
ignoring port security server authorization information, 193
implementing security ACL-based IPsec, 264
importing peer host public key from file, 220
importing public key from file, 223
importing SSH client host public key, 335
limiting port security secure MAC addresses, 189
logging out security portal authentication users, 142
maintaining 802.1X, 93
maintaining AAA HWTCACCS, 39
maintaining AAA RADIUS, 33
maintaining ARP attack detection, 423
maintaining crypto engine, 443
maintaining IP source guard (IPSG), 405
maintaining IPsec IKEv2, 318
maintaining IPv4 source guard (IPv4SG), 405
maintaining IPv6 ND attack defense RA guard, 482
maintaining IPv6 ND attack detection, 479
maintaining IPv6 source guard (IPv6SG), 405
maintaining MAC authentication, 115
maintaining MACsec, 469
maintaining security IPSec, 280
maintaining security IPsec IKE, 301
maintaining security password control, 213
maintaining security portal authentication, 145
obtaining PKI certificate, 234
troubleshooting PKI local certificate request failure, 255
troubleshooting PKI storage path set failure, 258
troubleshooting port security mode cannot be set, 204
troubleshooting port security secure MAC addresses, 205
troubleshooting security IPsec IKE negotiation failure (no proposal match), 304
troubleshooting security IPsec IKE negotiation failure (no proposal or keychain specified correctly), 304
troubleshooting security IPsec SA negotiation failure (invalid identity info), 305
troubleshooting security IPsec SA negotiation failure (no transform set match), 305
troubleshooting security portal authentication cannot log out users (access device), 182
troubleshooting security portal authentication cannot log out users (RADIUS server), 183
troubleshooting security portal authentication no page pushed for users, 182
troubleshooting security portal authentication users cannot log in (re-DHCP), 184
troubleshooting security portal authentication users logged out still exist on server, 183
verifying PKI certificate, 235
verifying PKI certificate verification (CRL checking), 235
verifying PKI certificate verification (w/o CRL checking), 236
working with SSH SFTP directories, 347
working with SSH SFTP files, 347
processing
parallel processing with 802.1X authentication, 110
profile
AAA NAS-ID profile configuration, 48
AAA RADIUS server status detection test profile, 23
IPsec IKEv2 configuration, 311
port security NAS-ID profile, 194
security IPsec IKE configuration, 293
security IPsec IPv6 routing protocol profile, 278
proposal
IPsec IKEv2 proposal configuration, 314
security IPsec IKE proposal, 295
protecting
ARP attack protection configuration, 411
ARP gateway protection, 428
MACsec protection parameter (MKA policy), 468
MACsec replay protection, 461, 468
protocols and standards
802.1X overview, 64
802.1X related protocols, 65
AAA, 13
AAA HWTACACS, 6, 13
AAA LDAP, 9, 13
AAA RADIUS, 2, 13
IPsec IKEv2, 310
IPsec security protocol 50 (ESP), 260
IPsec security protocol 51 (AH), 260
MACsec, 464
MFF, 433
security (IPsec IKE), 292
security (IPsec), 263
SSL configuration, 393, 394
SSL protocol stack, 393
public key
display, 221
file import, 223
FIPS compliance, 217
host public key display, 219
host public key export, 219
local host public key distribution, 219
local key pair creation, 217
local key pair destruction, 220
management, 217, 221
peer host public key configuration, 220
peer host public key entry, 221, 221
peer host public key import from file, 220
SSH client host public key configuration, 334
SSH password-publickey authentication, 329
SSH publickey authentication, 329
SSH Secure Telnet client configuration (publickey authentication-enabled), 365
SSH Secure Telnet server configuration (publickey authentication-enabled), 356
SSH SFTP client publickey authentication, 374
SSH user configuration, 335
Public Key Infrastructure. Use PKI
Q
QoS
security IPsec QoS pre-classify enable, 276
user profile configuration, 455
QoS or CAR parameters
configuring, 455
quiet
802.1X timer, 86
MAC authentication quiet timer, 108
IPv6 ND attack defense device role, 481
IPv6 ND attack defense RA guard configuration, 481, 483
IPv6 ND attack defense RA guard logging enable, 482
IPv6 ND attack defense RA guard policy, 481
PKI architecture, 227
PKI certificate, 226

RADIUS
802.1X EAP over RADIUS, 66
802.1X EAP relay enable, 81
802.1X RADIUS EAP termination enable, 81
802.1X RADIUS EAP-Message attribute, 66
802.1X RADIUS Message-Authentication attribute, 67
AAA configuration, 1, 17, 49
AAA implementation, 2
AAA local user configuration, 18
AAA MPLS L3VPN implementation, 13
AAA NAS-ID profile configuration, 48
AAA scheme, 18
accounting server parameters, 25
accounting-on configuration, 31
applying interface NAS-ID profile, 141
attributes, 14
authentication server, 24
client/server model, 2
common standard attributes, 14
display, 33
extended attributes, 6
H3C proprietary attributes, 15
HWTACACS/RADIUS differences, 7
information exchange security, 2
Login-Service attribute check method, 32
MAC authentication (RADIUS-based), 117
MAC authentication authorization VLAN, 104
MAC authentication method, 103
maintain, 33
outgoing packet source IP address, 29
packet exchange process, 3
packet format, 3
port security macAddressWithRadius, 187
port security NAS-ID profile, 194
protocols and standards, 13
request transmission attempts max, 27
scheme configuration, 22
scheme creation, 23
scheme VPN specification, 26
security policy server IP address, 32
server load sharing, 29
server status, 28
server status detection test profile, 23
session-control, 48
shared keys, 26
SNMP notification enable, 32
SSH user authentication+authorization, 52
SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
timer set, 30
traffic statistics units, 26
troubleshooting, 61
troubleshooting accounting error, 62
troubleshooting authentication failure, 61
troubleshooting packet delivery failure, 61
troubleshooting security portal authentication cannot log out users (RADIUS server), 183
user authentication methods, 2
username format, 26

rate limiting
ARP packet rate limit, 413

realtime
AAA HWTACACS realtime accounting timer, 38
AAA RADIUS realtime accounting timer, 30

rebooting
FIPS mode (automatic reboot), 452
FIPS mode (manual reboot), 452
FIPS mode entry (manual reboot), 450

record protocol (SSL), 393

recovering
security IPsec IKE invalid SPI recovery, 299

re-DHCP portal authentication mode, 126, 128

redundancy
IPsec anti-replay window and sequence number synchronization, 274

referencing
security portal authentication Web server, 132
registration authority. Use RA

relay agent
802.1X EAD assistant, 100
authorized ARP configuration (DHCP relay agent), 419
dynamic IPv4 source guard (IPv4SG)+DHCP relay agent configuration, 407

remote
802.1X authorization VLAN, 72
AAA remote accounting method, 12
AAA remote authentication, 12
AAA remote authentication configuration, 17
AAA remote authorization method, 12
Remote Authentication Dial-In User Service. Use RADIUS
removing
PKI certificate, 237
replaying
MACsec replay protection, 468
request
PKI certificate request abort, 234
requesting
PKI certificate request, 232
resource access restriction (portal authentication), 123
restrictions
ARP attack detection restricted forwarding, 422
ARP attack detection restricted forwarding configuration, 424
ARP scanning configuration, 426
FIPS configuration, 444
fixed ARP configuration, 426
IPsec policy configuration (IKE-based), 269
security IPsec configuration restrictions, 267
security portal authentication, 131
security user profile configuration, 454
SSH local key pair configuration, 332
SSH user configuration, 335
restrictions and guidelines
IPv6 ND attack detection, 478
Revest-Shamir-Adleman Algorithm. Use RSA RIPng
security IPsec RIPng, 285
roaming
security portal authentication roaming, 141
role
IPv6 ND attack defense device role, 481
routing
802.1X authentication configuration, 94
802.1X basic configuration, 94
802.1X configuration, 72, 80
802.1X guest VLAN configuration, 96
802.1X+ACL assignment configuration, 98
MFF configuration, 431, 433, 435
MFF configuration (manual-mode in ring network), 436
MFF configuration (manual-mode in tree network), 435
MFF periodic gateway probe, 434
security IPsec IPv6 routing protocol profile, 278
security IPsec IPv6 routing protocols configuration, 277

SSH configuration, 328
SSH server configuration, 331
RSA
host public key display, 219
host public key export, 219
peer host public key entry, 221
PKI certificate export, 237
PKI OpenCA server certificate request, 245
PKI RSA Keon CA server certificate request, 239
PKI Windows 2003 CA server certificate request, 242
public key import from file, 223
public key management, 217, 221
security IPsec IKE signature authentication, 291
SSH client host public key configuration, 334
SSH management parameters, 336
SSH Secure Telnet server configuration (publickey authentication-enabled), 356
SSH SFTP client publickey authentication, 374
rule
portal authentication file name rules, 143
portal authentication page file compression+saving rules, 144
portal authentication page request rules, 143
portal authentication post request rules, 143
security IPsec ACL rule keywords, 265
security portal authentication portal-free rule, 132
S
S/MIME (PKI secure email), 228
SA
IPsec IKEv2, 310
security IKE SA max number set, 300
security IPsec transform set, 265
troubleshooting IPsec SA negotiation failure (no transform set match), 326
troubleshooting IPsec SA negotiation failure (tunnel failure), 326
troubleshooting security IPsec SA negotiation failure (invalid identity info), 305
troubleshooting security IPsec SA negotiation failure (no transform set match), 305
SA (MACsec), 461
SAK (MACsec), 461
scheme
AAA, 18
AAA HWTACACS, 33
AAA HWTACACS scheme VPN, 36
AAA LDAP, 40
AAA LDAP scheme creation, 42
AAA RADIUS configuration, 22
AAA RADIUS scheme VPN, 26
SCP
client device configuration, 348
configuration, 381
configuration (Suite B), 383
file transfer+password authentication, 381
server connection establishment, 348
server connection establishment based on Suite B, 351
server enable, 333
SSH application, 328
secure shell. Use SSH
Secure Sockets Layer. Use SSL
Secure Telnet
client configuration (password authentication-enabled), 362
client configuration (publickey authentication-enabled), 365
client device configuration, 338
configuration, 353
configuration (128-bit Suite B), 367
server configuration (password authentication-enabled), 354
server configuration (publickey authentication-enabled), 356
server connection establishment, 339
server connection establishment based on Suite B, 342
SSH application, 328
SSH packet source IP address, 338
security
802.1X access control method, 82
802.1X authentication, 67, 68
802.1X authentication attempts max number for MAC authenticated users, 83
802.1X authentication configuration, 94
802.1X authentication request attempts max, 83
802.1X authentication server timeout timer, 83
802.1X authentication trigger, 85
802.1X Auth-Fail VLAN, 75, 89
802.1X authorization VLAN, 72
802.1X authorization VLAN configuration, 96
802.1X basic configuration, 94
802.1X concurrent port users max, 82
802.1X critical VLAN, 76, 90, 91
802.1X critical voice VLAN, 78, 91
802.1X display, 93
802.1X EAD assistant, 93, 100
802.1X EAP relay enable, 81
802.1X EAP termination enable, 81
802.1X EAP-Success packets sending, 91
802.1X enable, 80
802.1X guest VLAN, 74, 87
802.1X guest VLAN assignment delay, 88
802.1X guest VLAN configuration, 96
802.1X maintain, 93
802.1X mandatory port authentication domain, 86
802.1X online user handshake, 84
802.1X overview, 64
802.1X periodic online user reauthentication, 87
802.1X port authorization state, 82
802.1X related protocols, 65
802.1X supported domain name delimiters, 92
802.1X troubleshoot, 102
802.1X+ACL assignment configuration, 98
AAA concurrent login user max, 48
AAA configuration, 1, 17, 49
AAA device implementation, 11
AAA display, 49
AAA HWTACACS implementation, 6
AAA HWTACACS protocols and standards, 13
AAA HWTACACS scheme, 33, 34
AAA HWTACACS server SSH user, 49
AAA ISP domain accounting method, 47
AAA ISP domain attribute, 44
AAA ISP domain authentication method, 44
AAA ISP domain authorization method, 45
AAA ISP domain creation, 43
AAA ISP domain method, 43
AAA LDAP implementation, 9
AAA LDAP protocols and standards, 13
AAA LDAP scheme, 40
AAA LDAP server SSH user authentication, 56
AAA local user, 18
AAA MPLS L3VPN implementation, 13
AAA protocols and standards, 13
AAA RADIUS attributes, 14
AAA RADIUS implementation, 2
AAA RADIUS information exchange security mechanism, 2
AAA RADIUS protocols and standards, 13
AAA RADIUS scheme, 22
AAA RADIUS security policy server IP address, 32
AAA RADIUS server load sharing, 29
AAA RADIUS server SSH user authentication+authorization, 52
AAA RADIUS server status detection test profile, 23
AAA RADIUS session-control, 48
AAA scheme, 18
AAA SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50 about IPv6 ND attack defense, 477
ARP active acknowledgement, 417
ARP attack detection (source MAC-based), 414, 415
ARP attack detection configuration, 420
ARP attack detection configuration (user+packet validity check), 423
ARP attack detection display, 423
ARP attack detection logging enable, 422
ARP attack detection maintain, 423
ARP attack detection packet validity check, 421
ARP attack detection restricted forwarding, 422
ARP attack detection restricted forwarding configuration, 424
ARP attack detection user validity check configuration, 420
ARP attack protection (unresolvable IP attack), 411, 413
ARP attack protection blackhole routing (unresolvable IP attack), 412
ARP attack protection configuration, 411
ARP attack protection source suppression (unresolvable IP attack), 412
ARP filtering configuration, 428, 429
ARP gateway protection, 427, 428
ARP packet rate limit, 413
ARP packet source MAC consistency check, 416
ARP scanning, 426
ARP scanning configuration restrictions, 426 association. See SA
attack D&P configuration, 460
authorized ARP configuration, 417
authorized ARP configuration (DHCP relay agent), 419
authorized ARP configuration (DHCP server), 418
crypto engine configuration, 443
crypto engine display, 443
crypto engine maintain, 443
direct portal authentication configuration (local portal Web server), 144, 179
displaying IPsec, 280
displaying IPsec IKE, 301
displaying password control, 213
dynamic IPv4 source guard (IPv4SG)+DHCP relay agent configuration, 407
dynamic IPv4 source guard (IPv4SG)+DHCP snooping configuration, 406
dynamic IPv6 source guard (IPv6SG)+DHCPV6 snooping configuration, 409
expired password login, 207
FIPS configuration, 444, 449
FIPS configuration restrictions, 444
FIPS display, 449
FIPS mode configuration, 445
FIPS mode entry, 445
FIPS mode entry (automatic reboot), 449
FIPS mode entry (manual reboot), 450
FIPS mode exit, 447
FIPS mode exit (automatic reboot), 452
FIPS mode exit (manual reboot), 452
FIPS mode system changes, 446
FIPS self-test, 447
fixed ARP configuration, 426
fixed ARP configuration restrictions, 426
host public key export, 219
IP, 259, See also IPsec
IP source guard (IPSG) configuration, 400, 401, 405
IP source guard (IPSG) dynamic binding, 401
IP source guard (IPSG) static binding, 400
IPsec ACL, 265
IPsec ACL de-encapsulated packet check, 273
IPsec ACL-based implementation, 264
IPsec anti-replay, 274
IPsec anti-replay window and sequence number synchronization, 274
IPsec configuration, 280
IPsec encapsulation modes, 260
IPsec IKE (main mode/pre-shared key authentication), 301
IPsec IKE configuration, 290, 292, 301
IPsec IKE DPD, 298
IPsec IKE global identity information, 297
IPsec IKE invalid SPI recovery, 299
IPsec IKE keepalive, 298
IPsec IKE keychain, 296
IPsec IKE mechanism, 291
IPsec IKE NAT keepalive, 298
IPsec IKE profile configuration, 293
IPsec IKE proposal, 295
IPsec IKE SA max number set, 300
IPsec IKE SNMP notification, 300
IPsec IKEv2 configuration, 309, 311, 318
IPsec IKEv2 display, 318
IPsec IKEv2 maintain, 318
IPsec IKEv2 policy configuration, 314
IPsec IKEv2 profile configuration, 311
IPsec IKEv2 protocols and standards, 310
IPsec IPv6 routing protocol profile, 278
IPsec IPv6 routing protocols, 277
IPsec packet DF bit, 276
IPsec packet logging enable, 276
IPsec policy, 267
IPsec policy (IKE-based), 269
IPsec policy application to interface, 273
IPsec protocols, 260
IPsec QoS pre-classify enable, 276
IPsec RIPng, 285
IPsec SNMP notification, 279
IPsec source interface policy bind, 275
IPsec transform set, 265
IPsec tunnel establishment, 263
IPsec tunnel for IPv4 packets (IKE-based), 283
IPsec tunnel for IPv4 packets (manual), 280
IPv4 source guard (IPv4SG) configuration, 402
IPv4 source guard (IPv4SG) enable on interface, 402
IPv4 source guard (IPv4SG) static binding configuration, 402
IPv6 ND attack defense configuration, 477
IPv6 ND attack defense device role, 481
IPv6 ND attack defense RA guard configuration, 481, 483
IPv6 ND attack defense RA guard display, 482
IPv6 ND attack defense RA guard logging enable, 482
IPv6 ND attack defense RA guard maintain, 482
IPv6 ND attack defense RA guard policy, 481
IPv6 ND attack detection, 479
IPv6 source guard (IPv6SG) configuration, 403
IPv6 source guard (IPv6SG) enable on interface, 403
IPv6 source guard (IPv6SG) static binding configuration, 404
local host public key distribution, 219
local key pair creation, 217
local key pair destruction, 220
MAC authentication, 107, 115
MAC authentication (local), 115
MAC authentication (RADIUS-based), 117
MAC authentication ACL assignment, 105, 119
MAC authentication concurrent port users max, 109
MAC authentication configuration, 103
MAC authentication critical VLAN, 112
MAC authentication critical voice VLAN, 113
MAC authentication delay, 110, 110
MAC authentication display, 115
MAC authentication domain, 108
MAC authentication enable, 107
MAC authentication guest VLAN, 111
MAC authentication keep-online, 114
MAC authentication maintain, 115
MAC authentication multi-VLAN mode, 109
MAC authentication multi-VLAN mode configuration, 109
MAC authentication offline detection enable, 114
MAC authentication timer, 108
MAC authentication user account format, 108
MAC authentication user account policies, 103
MAC authentication user profile assignment, 106
MAC authentication VLAN assignment, 104
MAC security. Use MACsec
MACsec application mode, 462
MACsec configuration, 461, 465, 470
MACsec configuration (client-oriented), 470
MACsec configuration (device-oriented), 473
MACsec desire enable, 465
MACsec display, 469
MACsec maintain, 469
MACsec MKA enable, 465
MACsec MKA key server priority, 466
MACsec preshared key, 466
MACsec protection parameter (interface view), 467
MACsec protocols and standards, 464
MACsec secure association (SA), 461
MACsec secure association key (SAK), 461
MACsec services, 461
maintaining IPsec, 280
maintaining IPsec IKE, 301
maintaining password control, 213
MFF basic concepts, 432
MFF configuration, 431, 433, 435
MFF configuration (manual-mode in ring network), 436
MFF configuration (manual-mode in tree network), 435
MFF display, 434
MFF enable, 433
MFF network port, 432, 433
MFF operation modes, 432
MFF periodic gateway probe, 434
MFF protocols and standards, 433
MFF server IP address, 434
MFF user port, 432
NETCONF-over-SSH client user line, 334
NETCONF-over-SSH enable, 333
NETCONF-over-SSH+password authentication configuration, 390
parallel processing with 802.1X authentication, 110
password control, 209, 213
password control configuration, 206
password control enable, 209
password control global parameters, 210
password control local user parameters, 212
password control user group parameters, 211
password event logging, 208
password expiration, 207, 207
password history, 207
password not displayed, 208
password setting, 206
password updating, 207, 207
password user first login, 208
password user login control, 208
peer host public key configuration, 220
peer host public key entry, 221, 221
peer host public key import from file, 220
periodic MAC reauthentication, 106
PKI applications, 228
PKI architecture, 227
PKI CA policy, 227
PKI certificate export, 237
PKI certificate import/export, 248
PKI certificate obtain, 234
PKI certificate removal, 237
PKI certificate request, 232, 232
PKI certificate request (automatic), 233, 233
PKI certificate request (manual), 233
PKI certificate request abort, 234
PKI certificate verification, 235
PKI certificate verification (CRL checking), 235
PKI certificate verification (w/o CRL checking), 236
PKI certificate-based access control policy, 238
PKI configuration, 226, 229, 239
PKI CRL, 226
PKI digital certificate, 226
PKI display, 239
PKI domain configuration, 230, 230
PKI entity configuration, 229, 229
PKI MPLS L3VPN support, 228
PKI OpenCA server certificate request, 245
PKI operation, 227
PKI RSA Keon CA server certificate request, 239
PKI storage path, 236
PKI terminology, 226
PKI Windows 2003 CA server certificate request, 242
port. See port security
port security display, 195
portal authentication, 129
portal authentication BAS-IP, 140
portal authentication configuration, 123, 145
portal authentication cross-subnet, 156
portal authentication detection features, 136
portal authentication direct, 145
portal authentication domain, 135
portal authentication extended cross-subnet, 166
portal authentication extended direct, 159
portal authentication extended re-DHCP, 162
portal authentication fail-permit, 139
portal authentication local portal Web server, 125, 142
portal authentication local portal Web server configuration, 144
portal authentication logout, 142
portal authentication max number users, 135
portal authentication page customization, 142
portal authentication policy server, 124
portal authentication re-DHCP, 153
portal authentication roaming, 141
portal authentication security check function, 123
portal authentication server, 130
portal authentication server detection, 137
portal authentication server detection+user synchronization, 169
portal authentication source subnet, 133
portal authentication subnet, 134
portal authentication troubleshooting, 182
portal authentication types, 123
portal authentication user access, 132
portal authentication user online detection, 136
portal authentication user synchronization, 138
portal authentication Web server detection, 138
public key display, 221
public key import from file, 223
public key management, 217, 221
Secure Telnet client user line, 334
SSH authentication methods, 329
SSH client host public key configuration, 334
SSH configuration, 328
SSH display, 353
troubleshooting PKI storage path set failure, 258
uRPF configuration, 438, 442
uRPF display, 441
uRPF enable, 441

sending
802.1X EAP-Success packets, 91

server
802.1X authentication configuration, 94
802.1X authentication server timeout timer, 83
802.1X authorization VLAN configuration, 96
802.1X basic configuration, 94
802.1X configuration, 72, 80
802.1X guest VLAN configuration, 96
802.1X+ACL assignment configuration, 98
AAA HWTACACS quiet timer, 38
AAA HWTACACS response timeout timer, 38
AAA LDAP timeout period, 41
AAA RADIUS quiet timer, 30
AAA RADIUS response timeout timer, 30
AAA RADIUS server load sharing, 29
MAC authentication server timeout timer, 108
MACsec MKA key server priority, 466
MFF server IP address, 434
PKI OpenCA server certificate request, 245
PKI Windows 2003 CA server certificate request, 242
port security authorization information ignore, 193
portal authentication local portal Web server, 144
security portal authentication AAA server, 124
security portal authentication fail-permit, 139
security portal authentication policy server, 124
security portal authentication server, 124, 130
security portal authentication server detection, 137
security portal authentication system components, 123
security portal authentication Web server, 124, 130
security portal authentication Web server detection, 138
security portal authentication Web server reference, 132
SSL server policy configuration, 394

service
MACsec data encryption, 461
MACsec integrity check, 461
MACsec replay protection, 461

SFTP
client configuration (publickey authentication-enabled), 374
client device configuration, 342
configuration, 371
configuration (192-bit Suite B), 377
directories, 347
files, 347
help information display, 347
packet source IP address, 342
server configuration (password authentication-enabled), 372
server connection establishment, 343
server connection establishment based on Suite B, 346
server connection termination, 348
server enable, 333
SSH application, 328

AAA RADIUS session-control, 48
setting
802.1X authentication attempts max number for MAC authenticated users, 83
802.1X authentication request attempts max, 83
802.1X authentication timeout timers, 83
802.1X concurrent port users max, 82
802.1X port authorization state, 82
802.1X quiet timer, 86
AAA concurrent login user max, 48
AAA HWTACACS timer, 38
AAA HWTACACS traffic statistics unit, 37
AAA HWTACACS username format, 37
AAA LDAP server timeout period, 41
AAA RADIUS request transmission attempts max, 27
AAA RADIUS server status, 28
AAA RADIUS timer, 30
AAA RADIUS traffic statistics unit, 26
AAA RADIUS username format, 26
MAC authentication concurrent port users max, 109
port security mode, 189
security IPsec IKE SA max number, 300
security IPsec packet DF bit set, 276
security password, 206
security password control global parameters, 210
security password control local user parameters, 212
security password control user group parameters, 211
security portal authentication max number users, 135
security super password control parameters, 212

802.1X EAP-Success packets, 91
SSH management parameters, 336
shared key
AAA HWTACACS, 36
AAA RADIUS, 26
signature authentication (IKE), 291
SNMP
AAA RADIUS notifications, 32
port security enable, 195
security IPsec IKE SNMP notification, 300
security IPsec SNMP notification, 279
software
crypto engine configuration, 443
source
ARP attack detection (source MAC-based), 414, 415
ARP attack detection src-mac validity check, 421
security portal authentication portal-free rule, 132
security portal authentication subnet, 133
specifying
802.1X access control method, 82
802.1X mandatory port authentication domain, 86
802.1X supported domain name delimiters, 92
AAA HWTACACS accounting server, 35
AAA HWTACACS authentication server, 34
AAA HWTACACS authorization server, 34
AAA HWTACACS outgoing packet source IP address, 37
AAA HWTACACS scheme VPN, 36
AAA HWTACACS shared keys, 36
AAA LDAP authentication server, 42
AAA LDAP version, 40
AAA RADIUS accounting server parameters, 25
AAA RADIUS authentication server, 24
AAA RADIUS outgoing packet source IP address, 29
AAA RADIUS scheme VPN, 26
AAA RADIUS shared keys, 26
IPv6 ND attack defense device role, 481
MAC authentication domain, 108
MFF server IP address, 434
PKI storage path, 236
security portal authentication domain, 135
SSH Secure Telnet packet source IP address, 338
SSH server PKI domain, 337
SSH SFTP packet source IP address, 342
SSH2 algorithms, 351
SPI
security IPsec IKE invalid SPI recovery, 299
spoofing
uRPF configuration, 438, 442
uRPF enable, 441
SSH
AAA HWTACACS server SSH user, 49
AAA LDAP server SSH user authentication, 56
AAA RADIUS Login-Service attribute check method, 32
AAA RADIUS server SSH user authentication+authorization, 52
AAA SSH user local authentication+HWTACACS authorization+RADIUS accounting, 50
authentication methods, 329
client host public key configuration, 334
configuration, 328
display, 353
FIPS compliance, 331
how it works, 328
local key pair configuration restrictions, 332
management parameter configuration, 336
NETCONF, 328
NETCONF-over-SSH client user line, 334
NETCONF-over-SSH enable, 333
NETCONF-over-SSH+password authentication configuration, 390
peer host public key entry, 221
public key import from file, 223
public key management, 217, 221
SCP, 328
SCP client device, 348
SCP file transfer+password authentication, 381
SCP server connection establishment, 348
SCP server connection establishment based on Suite B, 351
SCP server enable, 333
Secure Copy. Use SCP
Secure FTP. Use SFTP
Secure Telnet, 328
Secure Telnet client configuration (password authentication-enabled), 362
Secure Telnet client configuration (publickey authentication-enabled), 365
Secure Telnet client device, 338
Secure Telnet client user line, 334
Secure Telnet configuration, 353
Secure Telnet configuration (128-bit Suite B), 367
Secure Telnet packet source IP address, 338
Secure Telnet server configuration (password authentication-enabled), 354
Secure Telnet server configuration (publickey authentication-enabled), 356
Secure Telnet server connection establishment, 339
Secure Telnet server connection establishment based on Suite B, 342
Secure Telnet server enable, 332
security SCP configuration, 381
security SCP configuration (Suite B), 383
server configuration, 331
server PKI domain, 337
SFTP, 328
SFTP client configuration (publickey authentication-enabled), 374
SFTP client device, 342
SFTP configuration, 371
SFTP configuration (192-bit Suite B), 377
SFTP directories, 347
SFTP files, 347
SFTP help information display, 347
SFTP packet source IP address, 342
SFTP server configuration (password authentication-enabled), 372
SFTP server connection establishment, 343
SFTP server connection establishment based on Suite B, 346
SFTP server connection termination, 348
SFTP server enable, 333
SSH2 algorithms, 351
SSH2 algorithms (encryption), 352
SSH2 algorithms (key exchange), 352
SSH2 algorithms (MAC), 353
SSH2 algorithms (public key), 352
support for Suite B, 330
user configuration, 335
user configuration restrictions, 335
versions, 328
X.509v3 certificate, 330
SSL
client policy configuration, 397
configuration, 393, 394
display, 399
FIPS compliance, 394
peer host public key entry, 221
PKI configuration, 226, 229, 239
PKI Web application, 228
protocol stack, 393
public key import from file, 223
public key management, 217, 221
security services, 393
server policy configuration, 394
static
IP source guard (IPSG) static binding, 400
IPv4 source guard (IPv4SG) configuration, 405
IPv4 source guard (IPv4SG) static binding configuration, 402
IPv6 source guard (IPv6SG) configuration, 408
IPv6 source guard (IPv6SG) static binding configuration, 404
port security static secure MAC address, 191
statistics
AAA HWTACACS traffic statistics units, 37
AAA RADIUS traffic statistics units, 26
sticky
port security secure MAC address, 191
storage
PKI storage path, 236
troubleshooting PKI storage path set failure, 258
subnetting
security portal authentication (cross-subnet for MPLS L3VPN), 177
security portal authentication cross-subnet configuration, 156
security portal authentication destination subnet, 134
security portal authentication extended cross-subnet, 166
security portal authentication source subnet, 133
Suite B
feature and software version compatibility, 331
super password control parameters, 212
suppressing
ARP attack protection source suppression (unresolvable IP attack), 412
synchronizing
security portal authentication server detection+user synchronization, 169
security portal authentication user synchronization, 138
system administration
attack D&P configuration, 460
FIPS configuration, 444, 449
FIPS mode configuration, 445
FIPS mode entry (automatic reboot), 449
FIPS mode entry (manual reboot), 450
FIPS mode exit (automatic reboot), 452
FIPS mode exit (manual reboot), 452
FIPS mode system changes, 446
IPsec IKEv2 configuration, 309, 311, 318
IPsec IKEv2 cookie challenge, 317
IPsec IKEv2 global parameters, 317
IPsec IKEv2 keychain, 316
IPsec IKEv2 proposal, 314
security portal authentication configuration, 123
SSH authentication methods, 329
SSH configuration, 328
SSH server local key pair generation, 332
TCP fragment attack prevention, 460

T
TCP
AAA HWTACACS implementation, 6
fragment attack prevention configuration, 460
SSL configuration, 393, 394

Telnet
security SSH Secure Telnet server connection establishment based on Suite B, 342
SSH Secure Telnet client configuration (password authentication-enabled), 362
SSH Secure Telnet client configuration (publickey authentication-enabled), 365
SSH Secure Telnet client device, 338
SSH Secure Telnet configuration, 353
SSH Secure Telnet configuration (128-bit Suite B), 367
SSH Secure Telnet packet source IP address, 338
SSH Secure Telnet server configuration (password authentication-enabled), 354
SSH Secure Telnet server configuration (publickey authentication-enabled), 356
SSH Secure Telnet server connection establishment, 339
terminal
AAA RADIUS Login-Service attribute check method, 32
terminating
SSH SFTP server connection, 348
testing
AAA RADIUS server status detection test profile, 23
FIPS conditional self-test, 447
FIPS power-up self-test, 447
FIPS triggered self-test, 447
TFTP
local host public key distribution, 219
time
security IPsec IKE negotiation (time-based lifetime), 261
timeout
802.1X authentication timeout, 83
MAC authentication server timeout, 108
timer
802.1X authentication timeout, 83
802.1X quiet, 86
AAA HWTACACS realtime accounting, 38
AAA HWTACACS server quiet, 38
AAA HWTACACS server response timeout, 38
AAA RADIUS realtime accounting, 30
AAA RADIUS server quiet, 30
AAA RADIUS server response timeout, 30
MAC authentication offline detect, 108
MAC authentication quiet, 108
MAC authentication server timeout, 108
topology
MFF configuration (manual-mode in ring network), 436
MFF configuration (manual-mode in tree network), 435
traffic
AAA HWTACACS traffic statistics units, 37
AAA RADIUS traffic statistics units, 26
security IPsec configuration, 259, 280
security IPsec IKE negotiation (traffic-based lifetime), 261
security IPsec RIPng, 285
security IPsec tunnel for IPv4 packets (IKE-based), 283
security IPsec tunnel for IPv4 packets (manual), 280
traffic monitoring
MFF configuration, 431, 433, 435
MFF configuration (manual-mode in ring network), 436
MFF configuration (manual-mode in tree network), 435
transform set (IPsec), 265
Transmission Control Protocol. Use TCP
transporting
security IPsec encapsulation transport mode, 260
trapping
AAA RADIUS SNMP notification, 32
port security SNMP notification, 195
triggering
802.1X authentication trigger, 85
FIPS self-test, 449
troubleshooting
802.1X, 102
802.1X EAD assistant Web browser users, 102
AAA HWTACACS, 62
AAA LDAP, 62
AAA LDAP authentication failure, 62
AAA RADIUS, 61
AAA RADIUS accounting error, 62
AAA RADIUS authentication failure, 61
AAA RADIUS packet delivery failure, 61
IPsec IKEv2, 326
IPsec IKEv2 negotiation failure (no proposal match), 326
IPsec SA negotiation failure (no transform set match), 326
IPsec SA negotiation failure (tunnel failure), 326
MACsec, 476
PKI CA certificate import failure, 256
PKI CA certificate obtain failure, 254
PKI certificate export failure, 257
PKI configuration, 253
PKI CRL obtain failure, 255
PKI local certificate import failure, 257
PKI local certificate obtain failure, 254
PKI local certificate request failure, 255
PKI storage path set failure, 258
port security, 204
port security mode cannot be set, 204
port security secure MAC addresses, 205
security IPsec IKE, 304
security IPsec IKE negotiation failure (no proposal match), 304
security IPsec IKE negotiation failure (no proposal or keychain specified correctly), 304
security IPsec SA negotiation failure (invalid identity info), 305
security IPsec SA negotiation failure (no transform set match), 305
security portal authentication, 182
security portal authentication cannot log out users (access device), 182
security portal authentication cannot log out users (RADIUS server), 183
security portal authentication no page pushed for users, 182
security portal authentication users cannot log in (re-DHCP), 184
security portal authentication users logged out still exist on server, 183
tunneling
security IPsec configuration, 259, 280
security IPsec encapsulation tunnel mode, 260
security IPsec RIPv2, 285
security IPsec tunnel establishment, 263
security IPsec tunnel for IPv4 packets (IKE-based), 283
security IPsec tunnel for IPv4 packets (manual), 280
UDP
AAA RADIUS implementation, 2
AAA RADIUS packet format, 3
AAA RADIUS request transmission attempts max, 27
AAA RADIUS session-control, 48
uncontrolled port (802.1X), 64
unicast
802.1X unicast trigger mode, 67, 85
Unicast Reverse Path Forwarding. Use uRPF
updating
security passwords, 207, 207
uRPF
check modes, 438
display, 441
enable, 441
network application, 441
operation, 438
user
802.1X concurrent port users max, 82
802.1X periodic online user reauthentication, 87
AAA concurrent login user max, 48
AAA local user, 18
AAA management by ISP domains, 11
AAA management by user access types, 11
AAA user role authentication, 12
ARP attack detection configuration (user+packet validity check), 423
ARP attack detection user validity check, 420
port security client userLoginWithOUI, 198
port security userLogin 802.1X authentication mode, 187
port security userLoginSecure 802.1X authentication mode, 187
port security userLoginSecureExt 802.1X authentication mode, 187
portal authentication authenticated user redirection, 144
port authentication authenticated user redirection, 144
security portal authentication max number users, 135
security portal authentication roaming, 141
security portal authentication user access, 132
security portal authentication user online detection, 136
SSH user configuration, 335
user access
dynamic IPv4 source guard (IPv4SG)+DHCP relay agent configuration, 407
dynamic IPv4 source guard (IPv4SG)+DHCP snooping configuration, 406
dynamic IPv6 source guard (IPv6SG)+DHCPv6 snooping configuration, 409
IP source guard (IPSG) configuration, 400, 405
static IPv4 source guard (IPv4SG) configuration, 405
static IPv6 source guard (IPv6SG) configuration, 408
user account
MAC authentication user account format, 108
MAC authentication user account policies, 103
user authentication
security password control, 209, 213
security password control configuration, 206
security password control global parameters, 210
security password control local user parameters, 212
security password control user group parameters, 211
security password event logging, 208
security password expiration, 207, 207
security password expired login, 207
security password history, 207
security password max user account idle time, 208
security password not displayed, 208
security password setting, 206
security password updating, 207, 207
security password user first login, 208
security password user login attempt limit, 208
security password user login control, 208
security super password control parameters, 212
user profile
802.1X authentication+user profile assignment, 79
configuration, 454
configuration restrictions, 454
creating, 454
displaying, 455
MAC authentication user profile assignment, 106
user profile parameters
configuring, 455
username
AAA HWTACACS format, 37
AAA RADIUS format, 26
V
validating
MACsec validation mode, 468
validity check
ARP attack detection configuration (user+packet validity check), 423
ARP attack detection packet, 421
ARP attack detection user, 420
verifying
PKI certificate, 235
PKI certificate verification (w/o CRL checking), 236
PKI certificate with CRL checking, 235
version
AAA LDAP, 40
VLAN
802.1X Auth-Fail VLAN, 75, 89
802.1X authorization VLAN, 72
802.1X authorization VLAN configuration, 96
802.1X critical VLAN, 76, 90, 91
802.1X critical voice VLAN, 78, 91
802.1X EAP-Success packets sending, 91
802.1X guest VLAN, 74, 87
802.1X guest VLAN assignment delay, 88
802.1X guest VLAN configuration, 96
802.1X VLAN manipulation, 72
802.1X+ACL assignment configuration, 98
about IPv6 ND attack defense, 477
IP source guard (IPSG) configuration, 400, 401, 405
IPv6 ND attack defense configuration, 477
IPv6 ND attack defense RA guard configuration, 481, 483
IPv6 ND attack detection, 479
MAC authentication authorization VLAN, 104
MAC authentication critical VLAN, 105
MAC authentication critical VLAN configuration, 112
MAC authentication critical voice VLAN enable, 113
MAC authentication guest VLAN, 104, 111
MAC authentication VLAN assignment, 104
MFF configuration, 431, 433, 435
MFF configuration (manual-mode in ring network), 436
MFF configuration (manual-mode in tree network), 435
port security secure MAC address, 191
security portal authentication portal-free rule, 132
security portal authentication roaming, 141
static IPv4 source guard (IPv4SG) configuration, 405
static IPv6 source guard (IPv6SG) configuration, 408

VPN
AAA HWTACACS scheme VPN, 36
AAA MPLS L3VPN implementation, 13
AAA RADIUS scheme VPN, 26
PKI application, 228
security IPsec configuration, 259, 280
security IPsec RIPng, 285
security IPsec tunnel for IPv4 packets (IKE-based), 283
security IPsec tunnel for IPv4 packets (manual), 280
security portal authentication (cross-subnet for MPLS L3VPN), 177

W
WAPI
PKI configuration, 226, 229, 239

Web
direct portal authentication configuration (local portal Web server), 144, 179
PKI, 228
portal authentication local portal Web server, 125, 142, 144
portal authentication local portal Web server page customization, 125
portal authentication local portal Web server+client interaction protocols, 125
security portal authentication, 129
security portal authentication configuration, 123, 145
security portal authentication cross-subnet, 156
security portal authentication direct, 145
security portal authentication extended cross-subnet, 166
security portal authentication extended direct, 159
security portal authentication extended functions, 123
security portal authentication extended re-DHCP, 162
security portal authentication re-DHCP, 153
security portal authentication server detection+user synchronization, 169
security portal authentication system components, 123
security portal authentication Web server, 124, 130
security portal authentication Web server detection, 138
security portal authentication Web server reference, 132
troubleshooting 802.1X EAD assistant browser users, 102

Windows
2000 PKI CA server SCEP add-on, 229
2000 PKI entity configuration, 229
2003 PKI CA server certificate request, 242

WLAN
802.1X overview, 64
port security client
macAddressElseUserLoginSecure, 201
port security client userLoginWithOUI, 198
port security configuration, 185, 188, 196
port security MAC address autoLearn, 196
working with
SSH SFTP directories, 347
SSH SFTP files, 347

X
X.500
AAA LDAP implementation, 9