HP 5120 EI Switch Series

Security

Configuration Guide

Part number: 5998-1800

Software version: Release 2220

Document version: 6W100-20130810

Legal and notice information

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

Configuring AAA

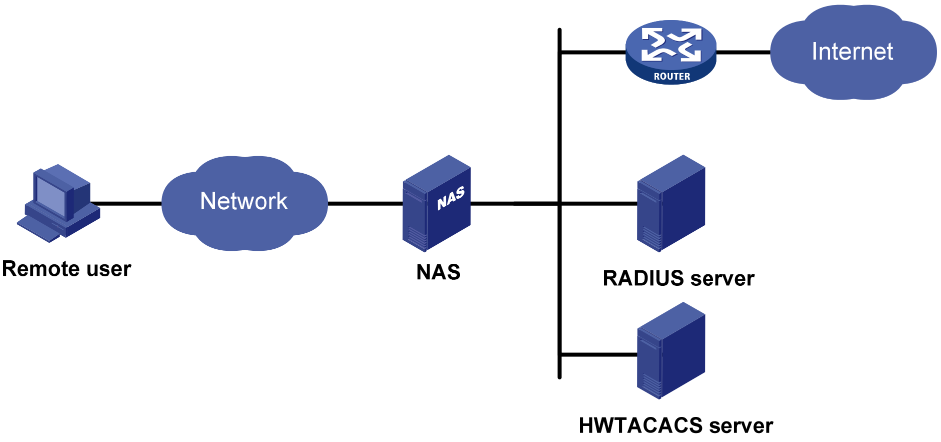
AAA overview

Authentication, Authorization, and Accounting (AAA) provides a uniform framework for implementing network access management. It can provide the following security functions:

- **Authentication**—Identifies users and determines whether a user is valid.
- **Authorization**—Grants different users different rights and controls their access to resources and services. For example, a user who has successfully logged in to the switch can be granted read and print permissions to the files on the switch.
- **Accounting**—Records all user network service usage information, including the service type, start time, and traffic. The accounting function not only provides the information required for charging, but also allows for network security surveillance.

AAA usually uses a client/server model. The client runs on the network access server (NAS), which is also referred to as the access device. The server maintains user information centrally. In an AAA network, a NAS is a server for users but a client for the AAA servers. See Figure 1.

Figure 1 Network diagram



When a user tries to log in to the NAS, use network resources, or access other networks, the NAS authenticates the user. The NAS can transparently pass the user's authentication, authorization, and accounting information to the servers. The RADIUS and HWTACACS protocols define how a NAS and a remote server exchange user information between them.

In the network shown in Figure 1, there is a RADIUS server and an HWTACACS server. You can choose different servers for different security functions. For example, you can use the HWTACACS server for authentication and authorization, and the RADIUS server for accounting.

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

AAA can be implemented through multiple protocols. The switch supports using RADIUS and HWTACACS. RADIUS is often used in practice.

RADIUS

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

RADIUS uses UDP as the transport protocol. It uses UDP port 1812 for authentication and UDP port 1813 for accounting.

RADIUS was originally designed for dial-in user access. With the addition of new access methods, RADIUS has been extended to support additional access methods, such as Ethernet and ADSL. RADIUS provides access authentication and authorization services, and its accounting function collects and records network resource usage information.

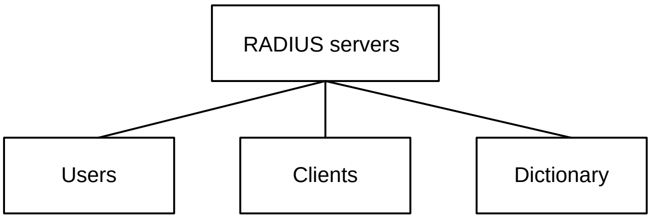
Client/server model

The RADIUS client runs on the NASs located throughout the network. It passes user information to designated RADIUS servers and acts on the responses (for example, rejects or accepts 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. It listens to connection requests, authenticates users, and returns user access control information (for example, rejecting or accepting the user access request) to the clients.

In general, the RADIUS server maintains the following databases: Users, Clients, and Dictionary.

Figure 2 RADIUS server components



- **Users**—Stores user information, such as 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.

Security and authentication mechanisms

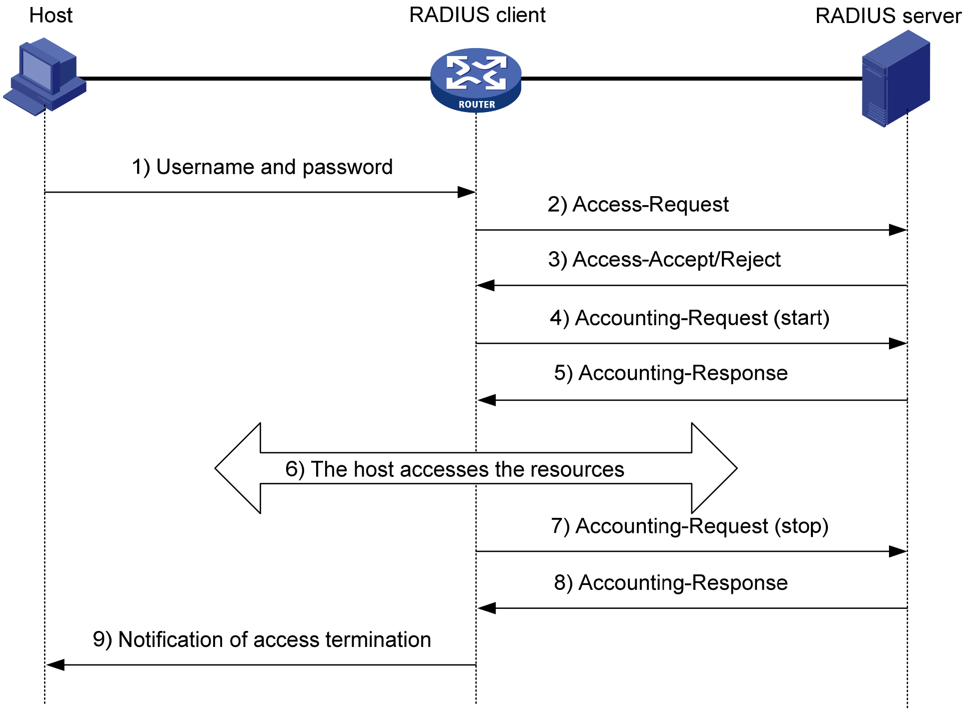
A RADIUS client and the RADIUS server use the shared key to authenticate RADIUS packets and encrypt user passwords that are exchanged between them. The keys are never transmitted over the network. This security mechanism improves the security of RADIUS communication and prevents user passwords from being intercepted on insecure networks.

A RADIUS server supports multiple user authentication methods. A RADIUS server can also act as the client of another AAA server to provide authentication proxy services.

Basic RADIUS message exchange process

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

Figure 3 Basic RADIUS message exchange process



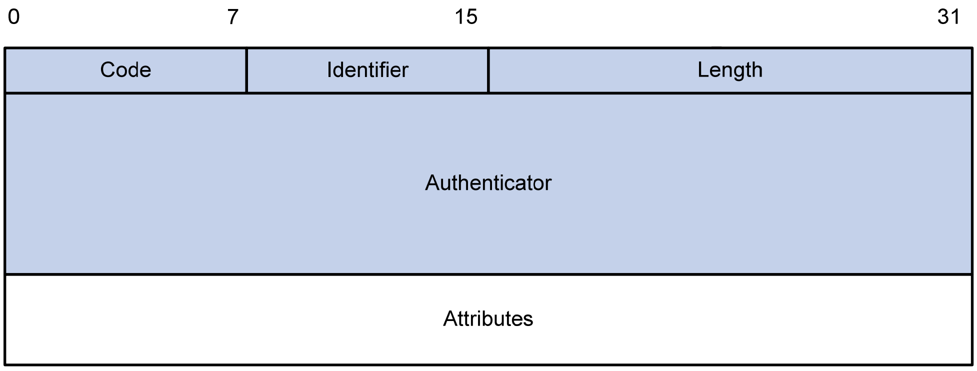
RADIUS operates in the following manner:

1. The host initiates a connection request that carries the user's username and password to the RADIUS client.
2. Having received the username and password, the RADIUS client sends an authentication request (Access-Request) to the RADIUS server, with the user password encrypted by using the Message-Digest 5 (MD5) algorithm and the shared key.
3. The RADIUS server authenticates the username and password. If the authentication succeeds, the server sends back an Access-Accept message containing the user's authorization information. If the authentication fails, the server returns an Access-Reject message.
4. The RADIUS client permits or denies the user according to the returned authentication result. If it permits the user, it sends a start-accounting request (Accounting-Request) to the RADIUS server.
5. The RADIUS server returns a start-accounting response (Accounting-Response) and starts accounting.
6. The user accesses the network resources.
7. The host requests the RADIUS client to tear down the connection and the RADIUS client sends a stop-accounting request (Accounting-Request) to the RADIUS server.
8. The RADIUS server returns a stop-accounting response (Accounting-Response) and stops accounting for the user.

RADIUS packet format

RADIUS uses UDP to transmit messages. To ensure smooth message exchange between the RADIUS server and the client, RADIUS uses a series of mechanisms, including the timer management mechanism, the retransmission mechanism, and the backup server mechanism. Figure 4 shows the RADIUS packet format.

Figure 4 RADIUS packet format



Descriptions of the fields are as follows:

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

Table 1 Main values of the Code field

Code	Packet type	Description
1	Access-Request	From the client to the server. A packet of this type carries 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.
2	Access-Accept	From the server to the client. If all the attribute values carried in the Access-Request are acceptable, the authentication succeeds, and the server sends an Access-Accept response.
3	Access-Reject	From the server to the client. If any attribute value carried in the Access-Request is unacceptable, the authentication fails and the server sends an Access-Reject response.
4	Accounting-Request	From the client to the server. A packet of this type carries 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.
5	Accounting-Response	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.

- The Identifier field (1 byte long) is used to match request and response packets and to detect duplicate request packets. Request and response packets of the same type have the same identifier.
- The Length field (2 bytes long) indicates the length of the entire packet, including the Code, Identifier, Length, Authenticator, and Attribute fields. Bytes beyond this length are considered padding and are ignored at the receiver. If the length of a received packet is less than this length, the packet is dropped. The value of this field is in the range of 20 to 4096.
- The Authenticator field (16 bytes long) is used to authenticate replies 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) carries the specific authentication, authorization, and accounting information that defines the configuration details of the request or response. This field may contain multiple attributes, each with three sub-fields:
    - **Type**—(1 byte long) Type of the attribute. It is in the range of 1 to 255. Commonly used RADIUS attributes are defined in RFC 2865, RFC 2866, RFC 2867, and RFC 2868. Table 2 shows a list of the attributes. For more information about commonly used standard RADIUS attributes, see "Commonly used standard RADIUS attributes."
    - **Length**—(1 byte long) Length of the attribute in bytes, including the Type, Length, and Value fields.
    - **Value**—(Up to 253 bytes) Value of the attribute. Its format and content depend on the Type and Length fields.

Table 2 Commonly used RADIUS attributes

No.	Attribute	No.	Attribute
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply-Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security

No.	Attribute	No.	Attribute
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-id
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

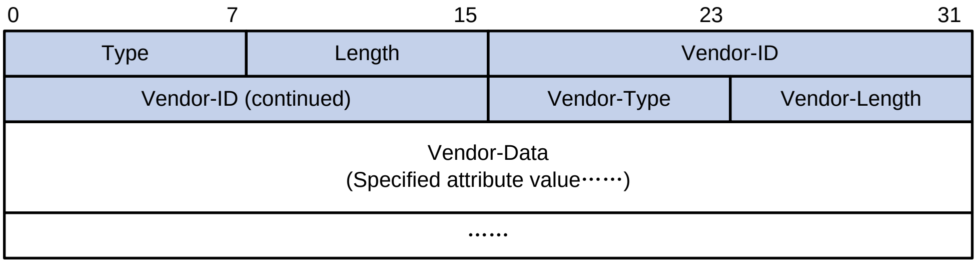
Extended RADIUS attributes

The RADIUS protocol features excellent extensibility. Attribute 26 (Vendor-Specific), an attribute defined by RFC 2865, allows a vendor to define extended attributes to implement functions that the standard RADIUS protocol does not provide.

A vendor can encapsulate multiple sub-attributes in the type-length-value (TLV) format in RADIUS packets for extension of applications. As shown in Figure 5, a sub-attribute encapsulated in Attribute 26 consists of the following parts:

- **Vendor-ID**—Indicates the ID of the vendor. Its most significant byte is 0, and the other three bytes contains a code that is compliant to RFC 1700. For more information about the proprietary RADIUS sub-attributes of HP, see "HP proprietary RADIUS sub-attributes."
- **Vendor-Type**—Indicates the type of the sub-attribute.
- **Vendor-Length**—Indicates the length of the sub-attribute.
- **Vendor-Data**—Indicates the contents of the sub-attribute.

Figure 5 Segment of a RADIUS packet containing an extended attribute



HWTACACS

HW Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC 1492). Similar to RADIUS, it uses a client/server model for information exchange between the NAS and the HWTACACS server.

HWTACACS typically provides AAA services for Point-to-Point Protocol (PPP) users, Virtual Private Dial-up Network (VPDN) users, and terminal users. In a typical HWTACACS scenario, some terminal users log in to the NAS for operations. Working as the HWTACACS client, the NAS sends the usernames and passwords of the users to the HWTACACS sever for authentication. After passing authentication and being authorized, the users log in to the switch and performs operations, and the HWTACACS server records the operations that each user performs.

Differences between HWTACACS and RADIUS

HWTACACS and RADIUS both provide authentication, authorization, and accounting services. They have many features in common, such as using a client/server model, using shared keys for user information security, and providing flexibility and extensibility.

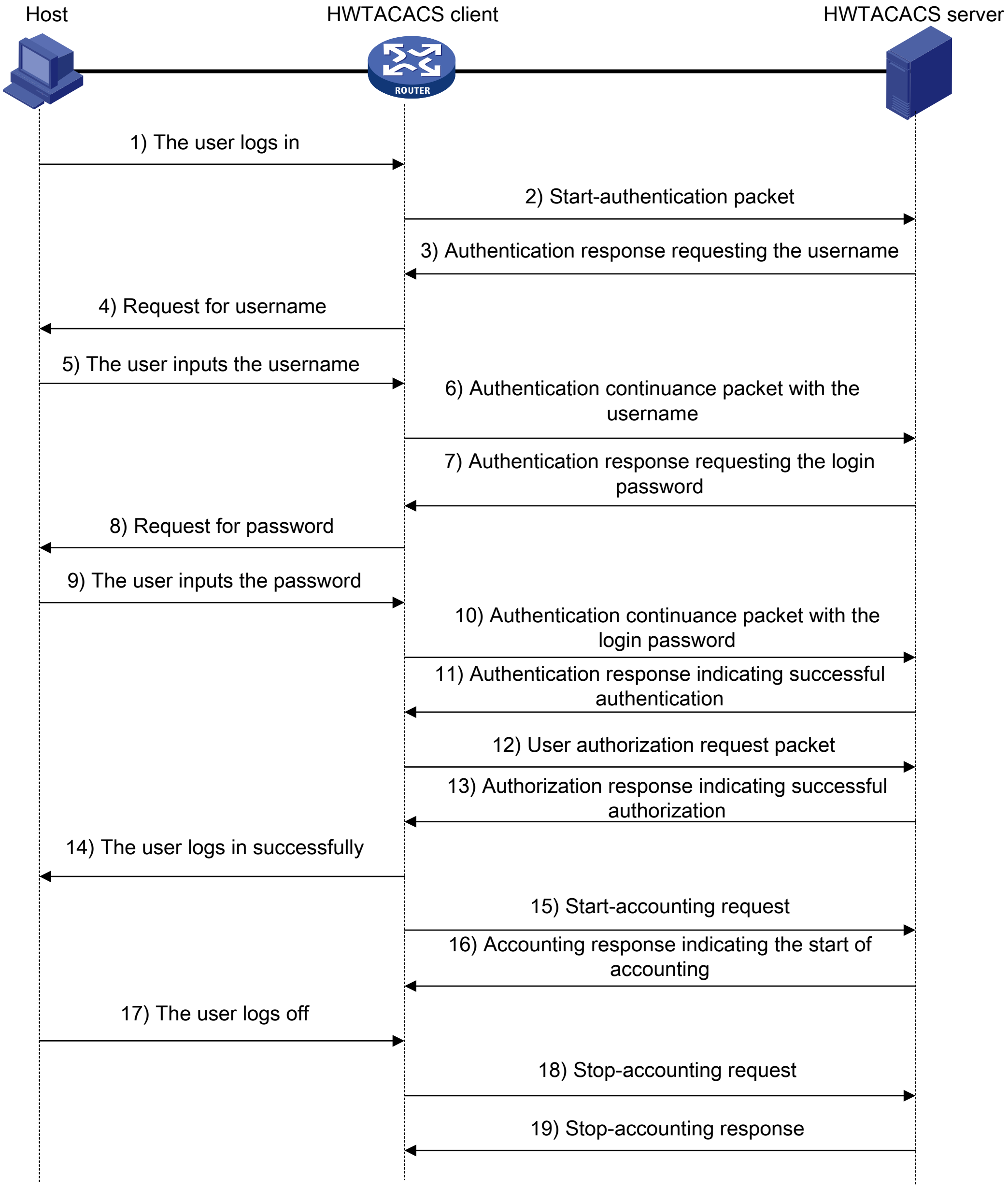
Table 3 Primary differences between HWTACACS and RADIUS

HWTACACS	**RADIUS**
Uses TCP, providing more reliable network transmission.	Uses UDP, providing higher transport efficiency.
Encrypts the entire packet except for the HWTACACS header.	Encrypts only the user password field in an authentication packet.
Protocol packets are complicated and authorization is independent of authentication. Authentication and authorization can be deployed on different HWTACACS servers.	Protocol packets are simple and the authorization process is combined with the authentication process.
Supports authorization of configuration commands. Which commands a user can use depends on both the user level and the AAA authorization. A user can use only commands that are at, or lower than, the user level and authorized by the HWTACACS server.	Does not support authorization of configuration commands. Which commands a user can use solely depends on the level of the user. A user can use all the commands at, or lower than, the user level.

Basic HWTACACS message exchange process

The following example describes how HWTACACS performs user authentication, authorization, and accounting for a Telnet user.

Figure 6 Basic HWTACACS message exchange process for a Telnet user


Host
HWTACACS client
ROUTER
HWTACACS server
1) The user logs in
2) Start-authentication packet
3) Authentication response requesting the username
4) Request for username
5) The user inputs the username
6) Authentication continuance packet with the username
7) Authentication response requesting the login password
8) Request for password
9) The user inputs the password
10) Authentication continuance packet with the login password
11) Authentication response indicating successful authentication
12) User authorization request packet
13) Authorization response indicating successful authorization
14) The user logs in successfully
15) Start-accounting request
16) Accounting response indicating the start of accounting
17) The user logs off
18) Stop-accounting request
19) Stop-accounting response

HWTACACS operates in the following manner:

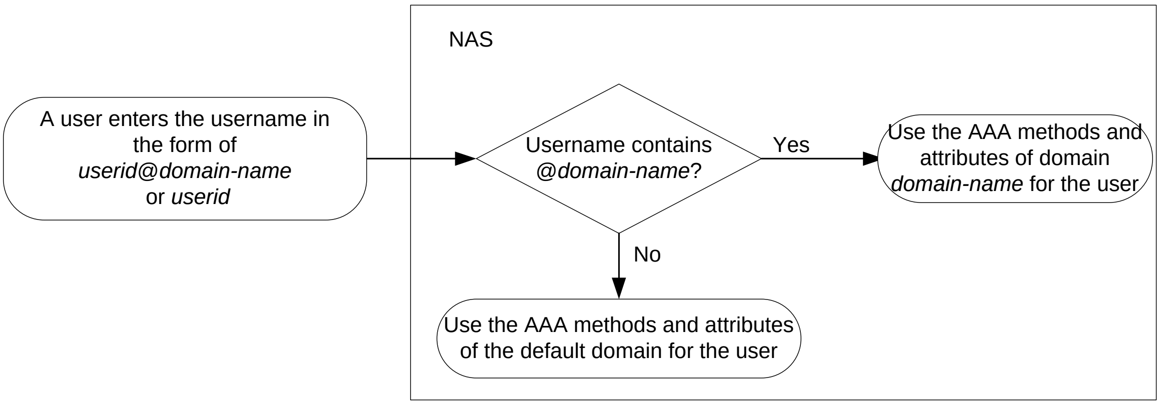
1. A Telnet user sends an access request to the HWTACACS client.
2. Upon receiving the request, the HWTACACS client sends a start-authentication packet to the HWTACACS server.
3. The HWTACACS server sends back an authentication response to request the username.
4. Upon receiving the response, the HWTACACS 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 carries the username.
7. The HWTACACS server sends back an authentication response, requesting the login password.
8. Upon receipt of the response, the HWTACACS client asks the user for the login password.

9. The user enters the password.
10. After receiving the login password, the HWTACACS client sends the HWTACACS server a continue-authentication packet that carries the login password.
11. The HWTACACS server sends back an authentication response to indicate that the user has passed authentication.
12. The HWTACACS client sends the user an authorization request packet to the HWTACACS server.
13. The HWTACACS server sends back the authorization response, indicating that the user is now authorized.
14. Knowing that the user is now authorized, the HWTACACS client pushes its configuration interface to the user.
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.

Domain-based user management

A NAS manages users based on Internet service provider (ISP) domains. On a NAS, each user belongs to one ISP domain. A NAS determines the ISP domain a user belongs to by the username entered by the user at login, as shown in Figure 7.

Figure 7 Determining the ISP domain of a user by the username


NAS
A user enters the username in the form of *userid@domain-name* or *userid*
Username contains *@domain-name*?
Yes
Use the AAA methods and attributes of domain *domain-name* for the user
No
Use the AAA methods and attributes of the default domain for the user

The authentication, authorization, and accounting of a user depends on the AAA methods configured for the domain to which the user belongs. If no specific AAA methods are configured for the domain, the default methods are used. By default, a domain uses local authentication, local authorization, and local accounting.

AAA allows you to manage users based on their access types:

- **LAN users**—Users on a LAN who must pass 802.1X or MAC address authentication to access the network.
- **Login users**—Users who want to log in to the switch, including SSH users, Telnet users, Web users, FTP users, and terminal users.

- **Portal users**—Users who must pass portal authentication to access the network.

In addition, AAA provides the following services for login users to enhance switch security:

- **Command authorization**—Enables the NAS to defer to the authorization server to determine whether a command entered by a login user is permitted for the user, making sure that login users execute only commands they are authorized to execute. For more information about command authorization, see *Fundamentals Configuration Guide*.
- **Command accounting**—Allows the accounting server to record all commands executed on the switch or all authorized commands successfully executed. For more information about command accounting, see *Fundamentals Configuration Guide*.
- **Level switching authentication**—Allows the authentication server to authenticate users who perform privilege level switching. As long as passing level switching authentication, users can switch their user privilege levels, without logging out and disconnecting current connections. For more information about user privilege level switching, see *Fundamentals Configuration Guide*.

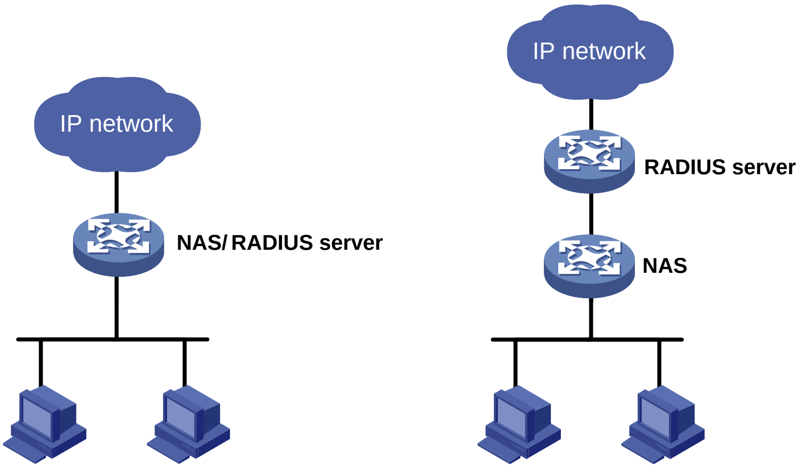
You can configure different authentication, authorization, and accounting methods for different types of users in a domain. See "Configuring AAA methods for ISP domains."

RADIUS server feature of the switch

Generally, the RADIUS server runs on a computer or workstation, and the RADIUS client runs on a NAS. A network device that supports the RADIUS server feature can also serve as the RADIUS server, working with RADIUS clients to implement user authentication, authorization, and accounting. As shown in Figure 8, the RADIUS server and client can reside on the same switch or different switches.

Using a network device as the RADIUS server simplifies networking and reduces deployment costs. This implementation is usually deployed on networks by using the clustering feature. In such a scenario, configure the RADIUS server feature on a management device at the distribution layer, so that the device functions as a RADIUS server to cooperate with cluster member switches at the access layer to provide user authentication and authorization services.

Figure 8 Devices functioning as a RADIUS server



The switch can serve as a RADIUS server to provide the following functions:

- User information management:

  You can create, modify, and delete user information, including the username, password, authority, lifetime, and user description.
- RADIUS client information management:

You can create and delete RADIUS clients, which are identified by IP addresses and configured with attributes such as a shared key. With a managed client range configured, the RADIUS server processes only the RADIUS packets from the clients within the management range. A shared key is used to ensure secure communication between a RADIUS client and the RADIUS server.

- RADIUS authentication and authorization

With the RADIUS server enabled, the switch checks whether or not the client of an incoming RADIUS packet is under its management. If yes, it verifies the packet validity by using the shared key, checks whether there is an account with the username, whether the password is correct, and whether the user attributes meet the requirements defined on the RADIUS server (for example, whether the account has expired). Then, the RADIUS server assigns the corresponding authority to the client if the authentication succeeds, or denies the client if the authentication fails.

NOTE:

A RADIUS server running the standard RADIUS protocol listens on UDP port 1812 for authentication requests, but an HP switch listens on UDP port 1645 instead when acting as the RADIUS server. Be sure to specify 1645 as the authentication port number on the RADIUS client when you use an HP switch as the RADIUS server.

Protocols and standards

The following protocols and standards are related to AAA, RADIUS, and HWTACACS:

- 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

No.	Attribute	Description
1	User-Name	Name of the user to be authenticated.
2	User-Password	User password for PAP authentication, present only in Access-Request packets in PAP authentication mode.
3	CHAP-Password	Digest of the user password for CHAP authentication, present only in Access-Request packets in CHAP authentication mode.
4	NAS-IP-Address	IP address for the server to identify a client. Usually, a client is identified by the IP address of the access interface on the NAS, namely the NAS IP address. This attribute is present in only Access-Request packets.
5	NAS-Port	Physical port of the NAS that the user accesses.
6	Service-Type	Type of service that the user has requested or type of service to be provided.
7	Framed-Protocol	Encapsulation protocol for framed access.

No.	Attribute	Description
8	Framed-IP-Address	IP address assigned to the user.
11	Filter-ID	Name of the filter list.
12	Framed-MTU	Maximum transmission unit (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, so as to avoid oversized EAP packets.
14	Login-IP-Host	IP address of the NAS interface that the user accesses.
15	Login-Service	Type of the service that the user uses for login.
18	Reply-Message	Text to be displayed to the user, which can be used by the server to indicate, for example, the reason of the authentication failure.
26	Vendor-Specific	Vendor specific attribute. A packet can contain one or more such proprietary attributes, each of which can contain one or more sub-attributes.
27	Session-Timeout	Maximum duration of service to be provided to the user before termination of the session.
28	Idle-Timeout	Maximum idle time permitted for the user before termination of the session.
31	Calling-Station-Id	User identification that the NAS sends to the server. For the LAN access service provided by an HP device, this attribute carries the MAC address of the user in the format HHHH-HHHH-HHHH.
32	NAS-Identifier	Identification that the NAS uses for indicating itself.
40	Acct-Status-Type	Type of the Accounting-Request packet. Possible values are as follows: • **1**—Start. • **2**—Stop. • **3**—Interim-Update. • **4**—Reset-Charge. • **7**—Accounting-On. (Defined in 3GPP, the 3rd Generation Partnership Project.) • **8**—Accounting-Off. (Defined in 3GPP.) • **9 to 14**—Reserved for tunnel accounting. • **15**—Reserved for failed.
45	Acct-Authentic	Authentication method used by the user. Possible values are as follows: • **1**—RADIUS. • **2**—Local. • **3**—Remote.
60	CHAP-Challenge	CHAP challenge generated by the NAS for MD5 calculation during CHAP authentication.

No.	Attribute	Description
61	NAS-Port-Type	Type of the physical port of the NAS that is authenticating the user. Possible values are as follows: • **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.
79	EAP-Message	Used for encapsulating EAP packets to allow the NAS to authenticate dial-in users via EAP without having to understand the EAP protocol.
80	Message-Authenticator	Used for authentication and checking of authentication packets to prevent spoofing Access-Requests. This attribute is used when RADIUS supports EAP authentication.
87	NAS-Port-Id	String for describing the port of the NAS that is authenticating the user.

HP proprietary RADIUS sub-attributes

No.	Sub-attribute	Description
1	Input-Peak-Rate	Peak rate in the direction from the user to the NAS, in bps.
2	Input-Average-Rate	Average rate in the direction from the user to the NAS, in bps.
3	Input-Basic-Rate	Basic rate in the direction from the user to the NAS, in bps.
4	Output-Peak-Rate	Peak rate in the direction from the NAS to the user, in bps.
5	Output-Average-Rate	Average rate in the direction from the NAS to the user, in bps.
6	Output-Basic-Rate	Basic rate in the direction from the NAS to the user, in bps.
15	Remanent_Volume	Remaining, available total traffic of the connection, in different units for different server types.
20	Command	Operation for the session, used for session control. It can be: • **1**—Trigger-Request. • **2**—Terminate-Request. • **3**—SetPolicy. • **4**—Result. • **5**—PortalClear.
24	Control_Identifier	Identification for retransmitted packets. For retransmitted packets of the same session, this attribute must take the same value. For retransmitted packets of different sessions, this attribute may take the same value. The client response of a retransmitted packet must also carry this attribute and the value of the attribute must be the same. For Accounting-Request packets of the start, stop, and interim update types, the Control-Identifier attribute is ineffective.

No.	Sub-attribute	Description
25	Result_Code	Result of the Trigger-Request or SetPolicy operation. A value of zero means the operation succeeded. Any other value means the operation failed.
26	Connect_ID	Index of the user connection.
28	Ftp_Directory	Working directory of the FTP user. For an FTP user, when the RADIUS client acts as the FTP server, this attribute is used to set the FTP directory on the RADIUS client.
29	Exec_Privilege	Priority of the EXEC user.
59	NAS_Startup_Timestamp	Startup time of the NAS in seconds, which is represented by the time elapsed after 00:00:00 on Jan. 1, 1970 (UTC).
60	Ip_Host_Addr	User IP address and MAC address carried 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.
61	User_Notify	Information to be sent from the server to the client transparently.
62	User_HeartBeat	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 device and is used for verifying the handshake messages from the 802.1X user. This attribute exists in only Access-Accept and Accounting-Request packets.
140	User_Group	User groups assigned after the SSL VPN user passes authentication. A user may belong to more than one user group. In this case, the user groups are delimited by semi-colons. This attribute is used for cooperation with the SSL VPN device.
141	Security_Level	Security level assigned after the SSL VPN user passes security authentication.
201	Input-Interval-Octets	Bytes input within a real-time accounting interval.
202	Output-Interval-Octets	Bytes output within a real-time accounting interval.
203	Input-Interval-Packets	Packets input within an accounting interval, in the unit set on the device.
204	Output-Interval-Packets	Packets output within an accounting interval, in the unit set on the device.
205	Input-Interval-Gigawords	Result of bytes input within an accounting interval divided by 4G bytes.
206	Output-Interval-Gigawords	Result of bytes output within an accounting interval divided by 4G bytes.
207	Backup-NAS-IP	Backup source IP address for sending RADIUS packets.
255	Product_ID	Product name.

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, you must complete these tasks on the NAS:

1. Configure the required AAA schemes.

- **Local authentication**—Configure local users and the related attributes, including the usernames and passwords of the users to be authenticated.
- **Remote authentication**—Configure the required RADIUS and HWTACACS schemes. You must configure user attributes on the servers accordingly.

2. Configure AAA methods for the users' ISP domains.
   - **Authentication method**—No authentication (**none**), local authentication (**local**), or remote authentication (**scheme**)
   - **Authorization method**—No authorization (**none**), local authorization (**local**), or remote authorization (**scheme**)
   - **Accounting method**—No accounting (**none**), local accounting (**local**), or remote accounting (**scheme**)

Figure 9 AAA configuration diagram

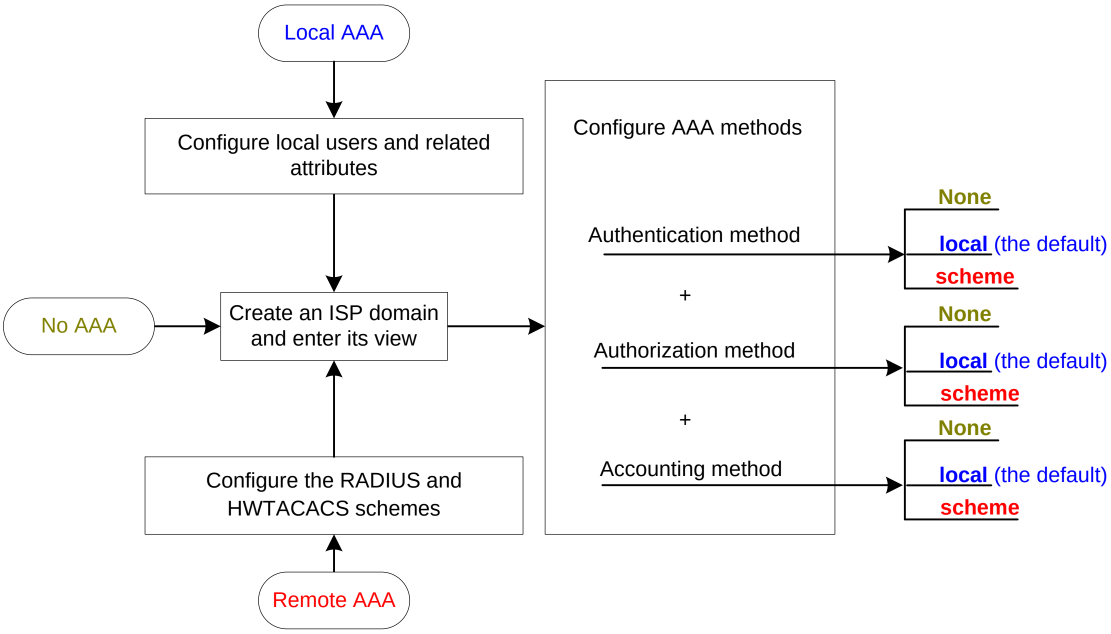


Table 4 AAA configuration task list

Task		Remarks
Configuring AAA schemes	Configuring local users	Required. Complete at least one task.
	Configuring RADIUS schemes	
	Configuring HWTACACS schemes	
Configuring AAA methods for ISP domains	Creating an ISP domain	Required.
	Configuring ISP domain attributes	Optional.
	Configuring AAA authentication methods for an ISP domain	Required. Complete at least one task.
	Configuring AAA authorization methods for an ISP domain	
	Configuring AAA accounting methods for an ISP domain	

Task	Remarks
Tearing down user connections	Optional.
Configuring a NAS ID-VLAN binding	Optional.
Configuring a switch as a RADIUS server	Optional.

NOTE:

To use AAA methods to control access of login users, you must configure the user interfaces to use AAA by using the **authentication-mode** command. For more information about the configuration command, see *Fundamentals Command Reference*.

Configuring AAA schemes

Configuring local users

To implement local user authentication, authorization, and accounting, you must create local users and configure user attributes on the switch. The local users and attributes are stored in the local user database on the switch. A local user is uniquely identified by a username. Configurable local user attributes are as follows:

- Service type.

  Types of 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, LAN access, portal, SSH, Telnet, terminal, and Web.
- User state.

  Indicates whether or not a local user can request network services. There are two user states: active and blocked. A user in active state can request network services, but a user in blocked state cannot.
- Maximum number of users using the same local user account.

  Indicates how many users can use the same local user account for local authentication.
- Validity time and expiration time.

  Indicates the validity time and expiration time of a local user account. A user must use a valid local user account to pass local authentication. For temporary network access requirements, you can create a guest account and specify a validity time and an expiration time for the account to control the validity of the account.
- User group.

  Each local user belongs to a local user group and bears all attributes of the group, such as the password control attributes and authorization attributes. For more information about local user group, see "Configuring user group attributes."
- Password control attributes.

  Password control attributes help you control the security of local users' passwords. Password control attributes include password aging time, minimum password length, and password composition policy.

  You can configure a password control attribute in system view, user group view, or local user view, making the attribute effective for all local users, all local users in a group, or only the local user. 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."

- Binding attributes.

  Binding attributes are used to control the scope of users. They 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 ISDN calling number, IP address, access port, MAC address, and native VLAN. For more information about binding attributes, see "Configuring local user attributes." Be cautious when deciding which binding attributes to configure for a local user.

- Authorization attributes.

  Authorization attributes indicate the rights that a user has after passing local authentication. Authorization attributes include the ACL, idle cut function, user level, user role, user profile, VLAN, and FTP/SFTP work directory. For more information about authorization attributes, see "Configuring local user attributes."

  Every configurable authorization attribute has its definite application environments and purposes. When you configure authorization attributes for a local user, consider which attributes are needed and which are not.

  You can configure an authorization attribute in user group view or local user view to make the attribute effective for all local users in the group or only for the local user. The setting of an authorization attribute in local user view takes precedence over that in user group view.

Local user configuration task list

Task	Remarks
Configuring local user attributes	Required
Configuring user group attributes	Optional
Displaying and maintaining local users and local user groups	Optional

Configuring local user attributes

Follow these guidelines when you configure local user attributes:

- If the user interface authentication mode (set by the **authentication-mode** command in user interface view) is AAA (**scheme**), which commands a login user can use after login depends on the privilege level authorized to the user. If the user interface authentication mode is password (**password**) or no authentication (**none**), which commands a login user can use after login depends on the level configured for the user interface (set by the **user privilege level** command in user interface view). For an SSH user using public key authentication, which commands are available depends on the level configured for the user interface. For more information about user interface authentication mode and user interface command level, see *Fundamentals Configuration Guide*.
- You can configure the user profile authorization attribute in local user view, user group view, and ISP domain view. The setting in local user view has the highest priority, and that in ISP domain view has the lowest priority. For more information about user profiles, see "Configuring a user profile."
- You cannot delete a local user who is the only security log manager in the system, nor can you change or delete the security log manager role of the user. To do so, you must specify a new security log manager first.

To configure local user attributes:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Add a local user and enter local user view.	**local-user** *user-name*	No local user exists by default.
3. Configure a password for the local user.	• In non-FIPS mode: **password** [[**hash**] { **cipher** | **simple** } *password*] • In FIPS mode: **password**	Optional. A local user with no password configured passes authentication after providing the valid local username and attributes. To enhance security, configure a password for each local user. If none of the parameters is specified, you enter the interactive mode to set a plaintext password. This interactive mode is available only on switches that support the password control feature.

4. Specify the service types for the local user.	• In non-FIPS mode:
	service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * | **portal** | **web** }
	• In FIPS mode:
	service-type { **lan-access** | { **ssh** | **terminal** } * | **portal** | **web** }
		By default, no service is authorized to a local user.

5. Place the local user to the state of active or blocked.	**state** { **active** | **block** }	Optional. When created, a local user is in active state by default, and the user can request network services.
6. Set the maximum number of concurrent users of the local user account.	**access-limit** *max-user-number*	Optional. By default, there is no limit to the maximum number of concurrent users of a local user account. The limit is effective only for local accounting, and is not effective for FTP users.
7. Configure the password control attributes for the local user.	• Set the password aging time: **password-control aging** *aging-time* • Set the minimum password length: **password-control length** *length* • Configure the password composition policy: **password-control composition type-number** *type-number* [**type-length** *type-length*]	Optional. By default, the local user uses password control attributes of the user group to which the local user belongs, and uses the global setting for any password control attribute that is not configured in the user group. For more information about password control configuration commands, see *Security Command Reference*.

Step	Command	Remarks
8. Configure the binding attributes for the local user.	**bind-attribute** { **ip** *ip-address* | **location port** *slot-number subslot-number port-number* | **mac** *mac-address* | **vlan** *vlan-id* } *	Optional. By default, no binding attribute is configured for a local user.
9. Configure the authorization attributes for the local user.	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minute* | **level** *level* | **user-profile** *profile-name* | **user-role** { **guest** | **guest-manager** | **security-audit** } | **vlan** *vlan-id* | **work-directory** *directory-name* } *	Optional. By default, no authorization attribute is configured for a local user. For LAN and portal users, only **acl**, **idle-cut**, **user-profile**, and **vlan** are supported. For SSH, terminal, and Web users, only **level** is supported. For FTP users, only **level** and **work-directory** are supported. For Telnet users, only **level** and **user-role** is supported. For other types of local users, no binding attribute is supported.
10. Set the validity time of the local user.	**validity-date** *time*	Optional. Not set by default.
11. Set the expiration time of the local user.	**expiration-date** *time*	Optional. Not set by default.
12. Assign the local user to a user group.	**group** *group-name*	Optional. By default, a local user belongs to the default user group **system**.

Configuring user group attributes

User groups simplify local user configuration and management. A user group consists of 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. Configurable user attributes include password control attributes and authorization attributes.

By default, every newly added local user belongs to the system default user group system and bears all attributes of the group. To change the user group to which a local user belongs, use the **user-group** command in local user view.

To configure attributes for a user group:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a user group and enter user group view.	**user-group** *group-name*	N/A

Step	Command	Remarks
3. Configure password control attributes for the user group.	- Set the password aging time: **password-control aging** *aging-time* - Set the minimum password length: **password-control length** *length* - Configure the password composition policy: **password-control composition type-number** *type-number* [**type-length** *type-length*]	Optional. By default, the user group uses global password control attribute settings. For more information about password control attributes configuration commands, see *Security Command Reference*.
4. Configure the authorization attributes for the user group.	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minute* | **level** *level* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *	Optional. By default, no authorization attribute is configured for a user group.
5. Set the guest attribute for the user group.	**group-attribute allow-guest**	Optional. By default, the guest attribute is not set for a user group, and guest users created by a guest manager through the Web interface cannot join the group.

Displaying and maintaining local users and local user groups

Task	Command	Remarks
Display local user information	**display local-user** [**idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **portal** | **ssh** | **telnet** | **terminal** | **web** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the user group configuration information.	**display user-group** [*group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Configuring RADIUS schemes

A RADIUS scheme specifies the RADIUS servers that the switch can cooperate with and defines a set of parameters that the switch uses to exchange information with the RADIUS servers. There may be authentication/authorization servers and accounting servers, or primary servers and secondary servers. The parameters include the IP addresses of the servers, the shared keys, and the RADIUS server type.

RADIUS scheme configuration task list

Task	Remarks
Creating a RADIUS scheme	Required
Specifying the RADIUS authentication/authorization servers	Required
Specifying the RADIUS accounting servers and the relevant parameters	Optional
Specifying the shared keys for secure RADIUS communication	Optional
Setting the username format and traffic statistics units	Optional
Setting the supported RADIUS server type	Optional
Setting the maximum number of RADIUS request transmission attempts	Optional
Setting the status of RADIUS servers	Optional
Specifying the source IP address for outgoing RADIUS packets	Optional
Setting timers for controlling communication with RADIUS servers	Optional
Configuring RADIUS accounting-on	Optional
Configuring the IP address of the security policy server	Optional
Configuring interpretation of RADIUS class attribute as CAR parameters	Optional
Enabling the trap function for RADIUS	Optional
Enabling the RADIUS client service	Optional
Setting the DSCP value for RADIUS packets	Optional
Displaying and maintaining RADIUS	Optional

Creating a RADIUS scheme

Before performing other RADIUS configurations, follow these steps to create a RADIUS scheme and enter RADIUS scheme view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a RADIUS scheme and enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	No RADIUS scheme exists by default.

NOTE:

A RADIUS scheme can be referenced by multiple ISP domains at the same time.

Specifying the RADIUS authentication/authorization servers

You can specify one primary authentication/authorization server and up to 16 secondary authentication/authorization servers for a RADIUS scheme. When the primary server is not available, a secondary server is used. In a scenario where redundancy is not required, specify only the primary server.

In RADIUS, user authorization information is piggybacked in authentication responses sent to RADIUS clients. There is no separate RADIUS authorization server.

You can enable the server status detection feature. With the feature, the switch periodically sends an authentication request to check whether or not the target RADIUS authentication/authorization server is reachable. If yes, the switch sets the status of the server to **active**. If not, the switch sets the status of the server to **block**. This feature can promptly notify authentication modules of latest server status information. For example, server status detection can work with the 802.1X critical VLAN feature, so that the switch can trigger 802.1X authentication for users in the critical VLAN immediately on detection of a reachable RADIUS authentication/authorization server.

Follow these guidelines when you specify RADIUS authentication/authorization servers:

- The IP addresses of the primary and secondary authentication/authorization servers for a scheme must be different from each other. Otherwise, the configuration fails.
- All servers for authentication/authorization and accounting, primary or secondary, must use IP addresses of the same IP version.
- You can specify a RADIUS authentication/authorization server as the primary authentication/authorization server for one scheme and as the secondary authentication/authorization server for another scheme at the same time.

To specify RADIUS authentication/authorization servers for a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Specify RADIUS authentication/authorization servers.	• Specify the primary RADIUS authentication/authorization server: **primary authentication** { *ip-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **probe username** *name* [**interval** *interval*]] * • Specify a secondary RADIUS authentication/authorization server: **secondary authentication** { *ip-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **probe username** *name* [**interval** *interval*]] *	Configure at least one command. No authentication/authorization server is specified by default.

Specifying the RADIUS accounting servers and the relevant parameters

You can specify one primary accounting server and up to 16 secondary accounting servers for a RADIUS scheme. When the primary server is not available, a secondary server is used. When redundancy is not required, specify only the primary server.

By setting the maximum number of real-time accounting attempts for a scheme, you make the switch disconnect users for whom no accounting response is received before the number of accounting attempts reaches the limit.

When the switch receives a connection teardown request from a host or a connection teardown notification from an administrator, it sends a stop-accounting request to the accounting server. You can enable buffering of non-responded stop-accounting requests to allow the switch to buffer and resend a stop-accounting request until it receives a response or the number of stop-accounting attempts reaches the configured limit. In the latter case, the switch discards the packet.

Follow these guidelines when you specify RADIUS accounting servers:

- The IP addresses of the primary and secondary accounting servers must be different from each other. Otherwise, the configuration fails.

- All servers for authentication/authorization and accountings, primary or secondary, must use IP addresses of the same IP version.
- If you delete an accounting server that is serving users, the switch can no longer send real-time accounting requests and stop-accounting requests for the users to that server, or buffer the stop-accounting requests.
- You can specify a RADIUS accounting server as the primary accounting server for one scheme and as the secondary accounting server for another scheme at the same time.
- RADIUS does not support accounting for FTP users.

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

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Specify RADIUS accounting servers.	• Specify the primary RADIUS accounting server: **primary accounting** { *ip-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key*] * • Specify a secondary RADIUS accounting server: **secondary accounting** { *ip-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key*] *	Configure at least one command. No accounting server is specified by default.
4. Set the maximum number of real-time accounting attempts.	**retry realtime-accounting** *retry-times*	Optional. The default setting is 5.
5. Enable buffering of stop-accounting requests to which no responses are received.	**stop-accounting-buffer enable**	Optional. Enabled by default.
6. Set the maximum number of stop-accounting attempts.	**retry stop-accounting** *retry-times*	Optional. The default setting is 500.

Specifying the shared keys for secure RADIUS communication

The RADIUS client and RADIUS server use the MD5 algorithm to authenticate packets exchanged between them and use shared keys for packet authentication and user passwords encryption. They must use the same key for the same type of communication.

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

To specify a shared key for secure RADIUS communication:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A

Step		Command	Remarks
3.	Specify a shared key for secure RADIUS authentication/authorization or accounting communication.	**key** { **accounting** | **authentication** [**cipher** | **simple**] } *key*	No shared key is specified by default.

NOTE:

A shared key configured on the switch must be the same as that configured on the RADIUS server.

Setting the username format and traffic statistics units

A username is usually in the format of *userid@isp-name*, where *isp-name* represents the name of the ISP domain the user belongs to and is used by the switch to determine which users belong to which ISP domains. However, some earlier RADIUS servers cannot recognize usernames that contain an ISP domain name. In this case, the switch must remove the domain name of each username before sending the username. You can set the username format on the switch for this purpose.

The switch periodically sends accounting updates to RADIUS accounting servers to report the traffic statistics of online users. For normal and accurate traffic statistics, make sure the unit for data flows and that for packets on the switch are consistent with those on the RADIUS server.

Follow these guidelines when you set the username format and the traffic statistics units for a RADIUS scheme:

- If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain. Otherwise, users using the same username but in different ISP domains are considered the same user.
- For level switching authentication, the **user-name-format keep-original** and **user-name-format without-domain** commands produce the same results. They make sure usernames sent to the RADIUS server carry no ISP domain name.

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

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3.	Set the format for usernames sent to the RADIUS servers.	**user-name-format** { **keep-original** | **with-domain** | **without-domain** }	Optional. By default, the ISP domain name is included in a username.
4.	Specify the unit for data flows or packets sent to the RADIUS servers.	**data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*	Optional. The default unit is **byte** for data flows and is **one-packet** for data packets.

Setting the supported RADIUS server type

The supported RADIUS server type determines the type of the RADIUS protocol that the switch uses to communicate with the RADIUS server. It can be standard or extended:

- **Standard**—Uses the standard RADIUS protocol, compliant to RFC 2865 and RFC 2866 or later.
- **Extended**—Uses the proprietary RADIUS protocol of HP.

When the RADIUS server runs on IMC, you must set the RADIUS server type to **extended**. When the RADIUS server runs third-party RADIUS server software, either RADIUS server type applies. For the switch to function as a RADIUS server to authenticate login users, you must set the RADIUS server type to **standard**.

To set the RADIUS server type:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Set the RADIUS server type.	**server-type** { **extended** | **standard** }	Optional. The default RADIUS server type is **standard**.

NOTE:

Changing the RADIUS server type restores the unit for data flows and that for packets that are sent to the RADIUS server to the defaults.

Setting the maximum number of RADIUS request transmission attempts

Because RADIUS uses UDP packets to transfer data, the communication process is not reliable. RADIUS uses a retransmission mechanism to improve the reliability. If a NAS sends a RADIUS request to a RADIUS server but receives no response after the response timeout timer (defined by the **timer response-timeout** command) expires, it retransmits the request. If the number of transmission attempts exceeds the specified limit but it still receives no response, it tries to communicate with other RADIUS servers in active state. If no other servers are in active state at the time, it considers the authentication or accounting attempt a failure. For more information about RADIUS server states, see "Setting the status of RADIUS servers."

To set the maximum number of RADIUS request transmission attempts for a scheme:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Set the maximum number of RADIUS request transmission attempts.	**retry** *retry-times*	Optional. The default setting is 3.

NOTE:

- The maximum number of transmission attempts of RADIUS packets multiplied by the RADIUS server response timeout period cannot be greater than 75 seconds.
- For more information about the RADIUS server response timeout period, see "Setting timers for controlling communication with RADIUS servers."

Setting the status of RADIUS servers

By setting the status of RADIUS servers to blocked or active, you can control which servers the switch communicates with for authentication, authorization, and accounting or turn to when the current servers are no longer available. In practice, you can specify one primary RADIUS server and multiple secondary RADIUS servers, with the secondary servers functioning as the backup of the primary servers. Generally, the switch chooses servers based on these rules:

- When the primary server is in active state, the switch communicates with the primary server. If the primary server fails, the switch changes the server's status to blocked and starts a quiet timer for the server, and then turns to a secondary server in active state (a secondary server configured earlier has a higher priority). If the secondary server is unreachable, the switch changes the server's status to blocked, starts a quiet timer for the server, and continues to check the next secondary server in active state. This search process continues until the switch finds an available secondary server or has checked all secondary servers in active state. If the quiet timer of a server expires or an authentication or accounting response is received from the server, the status of the server changes back to active automatically, but the switch does not check the server again during the authentication or accounting process. If no server is found reachable during one search process, the switch considers the authentication or accounting attempt a failure.
- Once the accounting process of a user starts, the switch keeps sending the user's real-time accounting requests and stop-accounting requests to the same accounting server. If you remove the accounting server, real-time accounting requests and stop-accounting requests for the user are no longer delivered to the server.
- If you remove an authentication or accounting server in use, the communication of the switch with the server soon times out, and the switch looks for a server in active state from scratch by checking any primary server first and then secondary servers in the order they are configured.
- When the primary server and secondary servers are all in blocked state, the switch communicates with the primary server. If the primary server is available, its status changes to active. Otherwise, its status remains to be blocked.
- If one server is in active state and all the others are in blocked state, the switch only tries to communicate with the server in active state, even if the server is unavailable.
- After receiving an authentication/accounting response from a server, the switch changes the status of the server identified by the source IP address of the response to active if the current status of the server is blocked.

The device does not change the status of an unreachable authentication or accounting server if the server quiet timer is set to 0. Instead, the device keeps the server status as active and sends authentication or accounting packets to another server in active state, so subsequent authentication or accounting packets can still be sent to that server. For more information about the server quiet timer, see "Setting timers for controlling communication with HWTACACS servers."

By default, the switch sets the status of all RADIUS servers to active. In cases such as a server failure, you can change the status of the server to blocked to avoid communication with the server.

To set the status of RADIUS servers in a RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A

Step	Command	Remarks

3. Set the RADIUS server status.	- Set the status of the primary RADIUS authentication/authorization 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/authorization server:
	state secondary authentication [**ip** *ipv4-address* | **ipv6** *ipv6-address*] { **active** | **block** }
	- Set the status of a secondary RADIUS accounting server:
	state secondary accounting [**ip** *ipv4-address* | **ipv6** *ipv6-address*] { **active** | **block** }
		Optional.
		By default, all servers in the RADIUS scheme are in active state.

NOTE:

- The server status set by the **state** command cannot be saved to the configuration file. After the switch restarts, the status of each server is restored to active.
- To display the states of the servers, use the **display radius scheme** command.

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 any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

Usually, the source address of outgoing RADIUS packets can be the IP address of the NAS's any interface that can communicate with the RADIUS server. In some special scenarios, however, you must change the source IP address.

You can specify a source IP address for outgoing RADIUS packets in RADIUS scheme view for a specific RADIUS scheme, or in system view for all RADIUS schemes. Before sending a RADIUS packet, a NAS selects a source IP address in the following order:

- Source IP address specified for the RADIUS scheme.
- Source IP address specified in system view.
- IP address of the outbound interface specified by the route.

To specify a source IP address for all RADIUS schemes:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify a source IP address for outgoing RADIUS packets.	**radius nas-ip** { *ip-address* | **ipv6** *ipv6-address* }	By default, the IP address of the outbound interface is used as the source IP address.

To specify a source IP address for a specific RADIUS scheme:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Specify a source IP address for outgoing RADIUS packets.	**nas-ip** { *ip-address* | **ipv6** *ipv6-address* }	By default, the IP address of the outbound interface is used as the source IP address.

Setting timers for controlling communication with RADIUS servers

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

- **Server response timeout timer** (**response-timeout**)—Defines the RADIUS request retransmission interval. After sending a RADIUS request (authentication/authorization or accounting request), the switch starts this timer. If the switch receives no response from the RADIUS server before this timer expires, it resends the request.
- **Server quiet timer** (**quiet**)—Defines the duration to keep an unreachable server in blocked state. If a server is not reachable, the switch changes the server's status to blocked, starts this timer for the server, and tries to communicate with another server in active state. After this timer expires, the switch changes the status of the server back to active.
- **Real-time accounting timer** (**realtime-accounting**)—Defines the interval at which the switch sends real-time accounting packets to the RADIUS accounting server for online users. To implement real-time accounting, the switch must periodically send real-time accounting packets to the accounting server for online users.

To set timers for controlling communication with RADIUS servers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Set the RADIUS server response timeout timer.	**timer response-timeout** *seconds*	Optional. The default RADIUS server response timeout timer is 3 seconds.
4. Set the quiet timer for the servers.	**timer quiet** *minutes*	Optional. The quiet timer is 5 minutes.
5. Set the real-time accounting timer.	**timer realtime-accounting** *minutes*	Optional. The default real-time accounting timer is 12 minutes.

- For a type of users, the maximum number of transmission attempts multiplied by the RADIUS server response timeout period must be less than the client connection timeout time and must not exceed 75 seconds. Otherwise, stop-accounting messages cannot be buffered, and the primary/secondary server switchover cannot take place. For example, the product of the two parameters must be less than 10 seconds for voice users, and less than 30 seconds for Telnet users because the client connection timeout period for voice users is 10 seconds and that for Telnet users is 30 seconds.

- When you configure the maximum number of RADIUS packet transmission attempts and the RADIUS server response timeout period, be sure to take the number of secondary servers into account. If the retransmission process takes too much time, the client connection in the access module may be timed out while the switch is trying to find an available server.
- When a number of secondary servers are configured, the client connections of access modules that have a short client connection timeout period may still be timed out during initial authentication or accounting, even if the packet transmission attempt limit and server response timeout period are configured with small values. In this case, the next authentication or accounting attempt may succeed because the switch has set the state of the unreachable servers to blocked and the time for finding a reachable server is shortened.
- Be sure to set the server quiet timer properly. Too short a quiet timer may result in frequent authentication or accounting failures because the switch has to repeatedly attempt to communicate with an unreachable server that is in active state.
- For more information about the maximum number of RADIUS packet transmission attempts, see "Setting the maximum number of RADIUS request transmission attempts."

Configuring RADIUS accounting-on

The accounting-on feature enables a switch to send accounting-on packets to the RADIUS server after it reboots, making the server log out users who logged in through the switch before the reboot. Without this feature, users who were online before the reboot cannot re-log in after the reboot, because the RADIUS server considers they are already online.

If a switch sends an accounting-on packet to the RADIUS server but receives no response, it resends the packet to the server at a particular interval for a specified number of times.

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

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3. Enable accounting-on and configure parameters.	**accounting-on enable** [**interval** *seconds* | **send** *send-times*] *	Disabled by default. The default interval is 3 seconds and the default number of send-times is 50.

NOTE:

The accounting-on feature requires the cooperation of the HP IMC network management system.

Configuring the IP address of the security policy server

The core of the HP EAD solution is integration and cooperation, and the security policy server is the management and control center. Using a collection of software, the security policy server provides functions such as user management, security policy management, security status assessment, security cooperation control, and security event audit.

The NAS checks 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, you must configure the IP address of the security policy server on the NAS. 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 the security policy server for a scheme:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3.	Specify a security policy server.	**security-policy-server** *ip-address*	No security policy server is specified by default.

Configuring interpretation of RADIUS class attribute as CAR parameters

According to RFC 2865, a RADIUS server assigns the RADIUS class attribute (attribute 25) to a RADIUS client. However, the RFC only requires the RADIUS client to send the attribute to the accounting server on an "as is" basis. It does not require the RADIUS client to interpret the attribute. Some RADIUS servers use the class attribute to deliver the assigned committed access rate (CAR) parameters. In this case, the switch must interpret the attribute as the CAR parameters to implement user-based traffic monitoring and controlling.

To configure the switch to interpret the RADIUS class attribute as CAR parameters:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter RADIUS scheme view.	**radius scheme** *radius-scheme-name*	N/A
3.	Interpret the class attribute as CAR parameters.	**attribute 25 car**	By default, RADIUS attribute 25 is not interpreted as CAR parameters.

NOTE:

Whether interpretation of RADIUS class attribute as CAR parameters is supported depends on two factors:

- Whether the switch supports CAR parameters assignment.
- Whether the RADIUS server supports assigning CAR parameters through the class attribute.

Enabling the trap function for RADIUS

With the trap function, a NAS sends a trap message when either of the following events occurs:

- The status of a RADIUS server changes. If a NAS receives no response to an accounting or authentication request before the specified maximum number of RADIUS request transmission attempts is exceeded, it considers the server unreachable, sets the status of the server to **block** and sends a trap message. If the NAS receives a response from a RADIUS server that it considers unreachable, the NAS considers that the RADIUS server is reachable again, sets the status of the server to **active**, and sends a trap message.
- The ratio of the number of failed transmission attempts to the total number of authentication request transmission attempts reaches the threshold. This threshold ranges from 1% to 100% and defaults to 30%. This threshold can only be configured through the MIB.

The failure ratio is generally small. If a trap message is triggered because the failure ratio is higher than the threshold, troubleshoot the configuration on and the communication between the NAS and the RADIUS server.

To enable the trap function for RADIUS:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the trap function for RADIUS.	**radius trap** { **accounting-server-down** | **authentication-error-threshold** | **authentication-server-down** }	Disabled by default.

Enabling the RADIUS client service

To receive and send RADIUS packets, enable the RADIUS client service on the device. If RADIUS is not required, disable the RADIUS client service to avoid attacks that exploit RADIUS packets.

To enable the RADIUS client service:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the RADIUS client service.	**radius client enable**	Optional. Enabled by default.

Setting the DSCP value for RADIUS packets

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the DSCP value for IPv4 RADIUS packets.	**radius dscp** *dscp-value*	Optional. The default DSCP value is 0.
3.	Set the DSCP value for IPv6 RADIUS packets.	**radius ipv6 dscp** *dscp-value*	Optional. The default DSCP value is 0.

Displaying and maintaining RADIUS

Task	Command	Remarks
Display the configuration information of RADIUS schemes.	**display radius scheme** [*radius-scheme-name*] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the statistics for RADIUS packets.	**display radius statistics** [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about buffered stop-accounting requests for which no responses have been received.	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear RADIUS statistics.	**reset radius statistics** [**slot** *slot-number*]	Available in user view

Task	Command	Remarks
Clear the buffered stop-accounting requests for which no responses have been receive.	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]	Available in user view

Configuring HWTACACS schemes

NOTE:

You cannot remove the HWTACACS schemes in use or change the IP addresses of the HWTACACS servers in use.

HWTACACS configuration task list

Task	Remarks
Creating an HWTACACS scheme	Required
Specifying the HWTACACS authentication servers	Required
Specifying the HWTACACS authorization servers	Optional
Specifying the HWTACACS accounting servers and the relevant parameters	Optional
Specifying the shared keys for secure HWTACACS communication	Required
Setting the username format and traffic statistics units	Optional
Specifying a source IP address for outgoing HWTACACS packets	Optional
Setting timers for controlling communication with HWTACACS servers	Optional
Displaying and maintaining HWTACACS	Optional

Creating an HWTACACS scheme

The HWTACACS protocol is configured on a per scheme basis. Before performing other HWTACACS configurations, follow these steps to create an HWTACACS scheme and enter HWTACACS scheme view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an HWTACACS scheme and enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	Not defined by default.

NOTE:

- Up to 16 HWTACACS schemes can be configured.
- A scheme can be deleted only when it is not referenced.

Specifying the HWTACACS authentication servers

You can specify one primary authentication server and up to one secondary authentication server for an HWTACACS scheme. When the primary server is not available, any secondary server is used. In a scenario where redundancy is not required, specify only the primary server.

Follow these guidelines when you specify HWTACACS authentication servers:

- An HWTACACS server can function as the primary authentication server of one scheme and as the secondary authentication server of another scheme at the same time.
- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

To specify HWTACACS authentication servers for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	N/A
3. Specify HWTACACS authentication servers.	• Specify the primary HWTACACS authentication server: **primary authentication** *ip-address* [*port-number*] • Specify the secondary HWTACACS authentication server: **secondary authentication** *ip-address* [*port-number*]	Configure at least one command. No authentication server is specified by default.

Specifying the HWTACACS authorization servers

You can specify one primary authorization server and up to one secondary authorization server for an HWTACACS scheme. When the primary server is not available, any secondary server is used. In a scenario where redundancy is not required, specify only the primary server.

Follow these guidelines when you specify HWTACACS authorization servers:

- 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.
- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

To specify HWTACACS authorization servers for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	N/A

Step	Command	Remarks
3. Specify HWTACACS authorization servers.	- Specify the primary HWTACACS authorization server: **primary authorization** *ip-address* [*port-number*] - Specify the secondary HWTACACS authorization server: **secondary authorization** *ip-address* [*port-number*]	Configure at least one command. No authorization server is specified by default.

Specifying the HWTACACS accounting servers and the relevant parameters

You can specify one primary accounting server and up to one secondary accounting server for an HWTACACS scheme. When the primary server is not available, any secondary server is used. In a scenario where redundancy is not required, specify only the primary server.

When the switch receives a connection teardown request from a host or a connection teardown command from an administrator, it sends a stop-accounting request to the accounting server. You can enable buffering of non-responded stop-accounting requests to allow the switch to buffer and resend a stop-accounting request until it receives a response or the number of stop-accounting attempts reaches the configured limit. In the latter case, the switch discards the packet.

Follow these guidelines when you specify HWTACACS accounting servers:

- 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.
- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.
- HWTACACS does not support accounting for FTP users.

To specify HWTACACS accounting servers and set relevant parameters for an HWTACACS scheme:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	N/A
3. Specify HWTACACS accounting servers.	- Specify the primary HWTACACS accounting server: **primary accounting** *ip-address* [*port-number*] - Specify the secondary HWTACACS accounting server: **secondary accounting** *ip-address* [*port-number*]	Configure at least one command. No accounting server is specified by default.
4. Enable buffering of stop-accounting requests to which no responses are received.	**stop-accounting-buffer enable**	Optional. Enabled by default.

Step		Command	Remarks
5.	Set the maximum number of stop-accounting attempts.	**retry stop-accounting** *retry-times*	Optional. The default setting is 100.

Specifying the shared keys for secure HWTACACS communication

The HWTACACS client and HWTACACS server use the MD5 algorithm to authenticate packets exchanged between them and use shared keys for packet authentication and user passwords encryption. They must use the same key for the same type of communication.

To specify a shared key for secure HWTACACS communication:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	N/A
3.	Specify a shared key for secure HWTACACS authentication, authorization, or accounting communication.	**key** { **accounting** | **authentication** | **authorization** } [**cipher** | **simple**] *key*	No shared key is specified by default.

NOTE:

A shared key configured on the switch must be the same as that configured on the HWTACACS server.

Setting the username format and traffic statistics units

A username is usually in the format of *userid@isp-name*, where *isp-name* represents the name of the ISP domain the user belongs to and is used by the switch to determine which users belong to which ISP domains. However, some HWTACACS servers cannot recognize usernames that contain an ISP domain name. In this case, the switch must remove the domain name of each username before sending the username. You can set the username format on the switch for this purpose.

The switch periodically sends accounting updates to HWTACACS accounting servers to report the traffic statistics of online users. For normal and accurate traffic statistics, make sure the unit for data flows and that for packets on the switch are consistent with those configured on the HWTACACS servers.

Follow these guidelines when you set the username format and the traffic statistics units for an HWTACACS scheme:

- If an HWTACACS server does not support a username that carries the domain name, configure the switch to remove the domain name before sending the username to the server.
- For level switching authentication, the **user-name-format keep-original** and **user-name-format without-domain** commands produce the same results. They make sure usernames sent to the HWTACACS server carry no ISP domain name.

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

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A

Step		Command	Remarks
2.	Enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	N/A
3.	Set the format for usernames sent to the HWTACACS servers.	**user-name-format** { **keep-original** | **with-domain** | **without-domain** }	Optional. By default, the ISP domain name is included in a username.
4.	Specify the unit for data flows or packets sent to the HWTACACS servers.	**data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*	Optional. The default unit is **byte** for data flows and is **one-packet** for data packets.

Specifying a 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. Upon receiving an HWTACACS packet, an HWTACACS server checks whether the source IP address of the packet is the IP address of any managed NAS. If yes, the server processes the packet. If not, the server drops the packet.

Usually, the source address of outgoing HWTACACS packets can be the IP address of the NAS's any interface that can communicate with the HWTACACS server. In some special scenarios, however, you must change the source IP address.

You can specify the source IP address for outgoing HWTACACS packets in HWTACACS scheme view for a specific HWTACACS scheme, or in system view for all HWTACACS schemes.

Before sending an HWTACACS packet, a NAS selects a source IP address in the following order:

- Source IP address specified for the HWTACACS scheme.
- Source IP address specified in system view.
- IP address of the outbound interface specified by the route.

To specify a source IP address for all HWTACACS schemes:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Specify a source IP address for outgoing HWTACACS packets.	**hwtacacs nas-ip** *ip-address*	By default, the IP address of the outbound interface is used as the source IP address.

To specify a source IP address for a specific HWTACACS scheme:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	N/A
3.	Specify a source IP address for outgoing HWTACACS packets.	**nas-ip** *ip-address*	By default, the IP address of the outbound interface is used as the source IP address.

Setting timers for controlling communication with HWTACACS servers

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

- **Server response timeout timer** (**response-timeout**)—Defines the HWTACACS request retransmission interval. After sending an HWTACACS request (authentication, authorization, or accounting request), the switch starts this timer. If the switch receives no response from the server before this timer expires, it resends the request.
- **Server quiet timer** (**quiet**)—Defines the duration to keep an unreachable server in blocked state. If a server is not reachable, the switch changes the server's status to blocked, starts this timer for the server, and tries to communicate with another server in active state. After this timer expires, the switch changes the status of the server back to active.
- **Real-time accounting timer** (**realtime-accounting**)—Defines the interval at which the switch sends real-time accounting updates to the HWTACACS accounting server for online users. To implement real-time accounting, the switch must send real-time accounting packets to the accounting server for online users periodically.

To set timers for controlling communication with HWTACACS servers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter HWTACACS scheme view.	**hwtacacs scheme** *hwtacacs-scheme-name*	N/A
3. Set the HWTACACS server response timeout timer.	**timer response-timeout** *seconds*	Optional. The default HWTACACS server response timeout timer is 5 seconds.
4. Set the quiet timer for the primary server.	**timer quiet** *minutes*	Optional. The default quiet timer for the primary server is 5 minutes.
5. Set the real-time accounting interval.	**timer realtime-accounting** *minutes*	Optional. The default real-time accounting interval is 12 minutes.

NOTE:

Consider the performance of the NAS and the HWTACACS server when you set the real-time accounting interval. A shorter interval requires higher performance. A shorter interval requires higher performance.

Displaying and maintaining HWTACACS

Task	Command	Remarks
Display the configuration information or statistics of HWTACACS schemes.	**display hwtacacs** [*hwtacacs-server-name* [**statistics**]] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Task	Command	Remarks
Display information about buffered stop-accounting requests for which no responses have been received.	**display stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name* [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear HWTACACS statistics.	**reset hwtacacs statistics** { **accounting** | **all** | **authentication** | **authorization** } [**slot** *slot-number*]	Available in user view
Clear buffered stop-accounting requests that get no responses.	**reset stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name* [**slot** *slot-number*]	Available in user view

Configuring AAA methods for ISP domains

You configure AAA methods for an ISP domain by referencing configured AAA schemes in ISP domain view. Each ISP domain has a set of default AAA methods, which are local authentication, local authorization, and local accounting by default and can be customized. If you do not configure any AAA methods for an ISP domain, the switch uses the system default AAA methods for authentication, authorization, and accounting of the users in the domain.

Configuration prerequisites

To use local authentication for users in an ISP domain, configure local user accounts (see "Configuring local user attributes") on the switch.

To use remote authentication, authorization, and accounting, create the required RADIUS, and HWTACACS, schemes as described in "Configuring RADIUS schemes," "Configuring HWTACACS schemes".

Creating an ISP domain

In a networking scenario with multiple ISPs, the switch may connect users of different ISPs, and users of different ISPs may have different user attributes, such as different username and password structures, different service types, and different rights. To distinguish the users of different ISPs, configure ISP domains, and configure different AAA methods and domain attributes for the ISP domains.

The switch can accommodate up to 16 ISP domains, including the system-defined ISP domain **system**. You can specify one of the ISP domains as the default domain.

On the switch, each user belongs to an ISP domain. If a user provides no ISP domain name at login, the switch considers the user belongs to the default ISP domain.

To create an ISP domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an ISP domain and enter ISP domain view.	**domain** *isp-name*	N/A

Step		Command	Remarks
3.	Return to system view.	**quit**	N/A
4.	Specify the default ISP domain.	**domain default enable** *isp-name*	Optional. By default, the default ISP domain is the system-defined ISP domain **system**.

NOTE:

To delete the ISP domain that is functioning as the default ISP domain, you must change it to a non-default ISP domain by using the **undo domain default enable** command.

Configuring ISP domain attributes

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

- **Domain status**—By placing the ISP domain to the active or blocked state, you allow or deny network service requests from users in the domain.
- **Maximum number of online users**—The switch controls the number of online users in a domain to ensure the system performance and service reliability.
- **Idle cut**—This function enables the switch to check the traffic of each online user in the domain at the idle timeout interval, and to log out any user in the domain whose traffic during the idle timeout period is less than the specified minimum traffic.
- **Self-service server location**—By using the information defined in this attribute, users can access the self-service server to manage their own accounts and passwords. A self-service RADIUS server, such as IMC, is required for the self-service server location function to work.
- **Default authorization user profile**—If a user passes authentication but is authorized with no user profile, the switch authorizes the default user profile of the ISP domain to the user and restricts the user's behavior based on the profile. For more information about user profiles, see "Configuring a user profile."

To configure ISP domain attributes:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter ISP domain view.	**domain** *isp-name*	N/A
3.	Place the ISP domain to the state of active or blocked.	**state** { **active** | **block** }	Optional. By default, an ISP domain is in active state, and users in the domain can request network services.
4.	Specify the maximum number of online users in the ISP domain.	**access-limit enable** *max-user-number*	Optional. No limit by default.
5.	Configure the idle cut function.	**idle-cut enable** *minute* [*flow*]	Optional. Disabled by default. This command is effective for only LAN users and portal users.

Step	Command	Remarks
6. Enable the self-service server location function and specify the URL of the self-service server.	**self-service-url enable** *url-string*	Optional. Disabled by default.
7. Specify the default authorization user profile.	**authorization-attribute user-profile** *profile-name*	Optional. By default, an ISP domain has no default authorization user profile.

Configuring AAA authentication methods for an ISP domain

In AAA, authentication, authorization, and accounting are separate processes. Authentication refers to the interactive authentication process of username/password/user information during an access or service request. The authentication process does not send authorization information to a supplicant or trigger accounting.

AAA supports the following authentication methods:

- **No authentication** (**none**)—All users are trusted and no authentication is performed. Generally, do not use this method.
- **Local authentication** (**local**)—Authentication is performed by the NAS, which is configured with the 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** (**scheme**)—The NAS cooperates with a RADIUS, or HWTACACS server to authenticate users. Remote authentication provides centralized information management, high capacity, high reliability, and support for centralized authentication service for multiple NASs. You can configure local or no authentication as the backup method, which is used when the remote server is not available. No authentication can only be configured for LAN users as the backup method of remote authentication.

You can configure AAA authentication to work alone without authorization and accounting. By default, an ISP domain uses the local authentication method.

Before configuring authentication methods, complete the following tasks:

1. For RADIUS or HWTACACS authentication, configure the RADIUS or HWTACACS scheme to be referenced first. The local and none authentication methods do not require a scheme.
2. 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, limiting the authentication protocols that can be used for access.
3. Determine whether to configure an authentication method for all access types or service types.

Follow these guidelines when you configure AAA authentication methods for an ISP domain:

- The authentication method specified with the **authentication default** command is for all types of users and has a priority lower than that for a specific access type.
- With an authentication method that references a RADIUS scheme, AAA accepts only the authentication result from the RADIUS server. The Access-Accept message from the RADIUS server also carries the authorization information, but the authentication process ignores the information.

- If you specify the **radius-scheme** *radius-scheme-name* **local**, **hwtacacs-scheme** *hwtacacs-scheme-name* **local** option when you configure an authentication method, local authentication is the backup method and is used only when the remote server is not available.
- If you specify only the **local** or **none** keyword in an authentication method configuration command, the switch has no backup authentication method and performs only local authentication or does not perform any authentication.
- If the method for level switching authentication references an HWTACACS scheme, the switch uses the login username of a user for level switching authentication of the user by default. If the method for level switching authentication references a RADIUS scheme, the system uses the username configured for the corresponding privilege level on the RADIUS server for level switching authentication, rather than the login username. A username configured on the RADIUS server is in the format of **$enab***level***$**, where *level* specifies the privilege level to which the user wants to switch. For example, if user **user1** of domain **aaa** wants to switch the privilege level to 3, the system uses **$enab3@aaa$** for authentication when the domain name is required and uses **$enab3$** for authentication when the domain name is not required.

To configure AAA authentication methods for an ISP domain:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter ISP domain view.	**domain** *isp-name*	N/A
3.	Specify the default authentication method for all types of users.	**authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The default authentication method is **local** for all types of users.
4.	Specify the authentication method for LAN users.	**authentication lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local** | **none**] }	Optional. The default authentication method is used by default.
5.	Specify the authentication method for login users.	**authentication login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The default authentication method is used by default.
6.	Specify the authentication method for portal users.	**authentication portal** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The default authentication method is used by default.
7.	Specify the authentication method for privilege level switching.	**authentication super** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **radius-scheme** *radius-scheme-name* }	Optional. The default authentication method is used by default.

Configuring AAA authorization methods for an ISP domain

In AAA, authorization is a separate process at the same level as authentication and accounting. Its responsibility is to send authorization requests to the specified authorization servers and to send authorization information to users after successful authorization. Authorization method configuration is optional in AAA configuration.

AAA supports the following authorization methods:

- **No authorization** (**none**)—The NAS performs no authorization exchange. After passing authentication, non-login users can access the network, FTP users can access the root directory of the NAS, and other login users have only the rights of Level 0 (visiting).
- **Local authorization** (**local**)—The NAS performs authorization according to the user attributes configured for users.
- **Remote authorization** (**scheme**)—The NAS cooperates with a RADIUS, or HWTACACS 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 carried in the Access-Accept message. HWTACACS authorization is separate from HWTACACS authentication, and the authorization information is carried in the authorization response after successful authentication. You can configure local authorization or no authorization as the backup method, which is used when the remote server is not available.

Before configuring authorization methods, complete the following tasks:

1. For HWTACACS authorization, configure the HWTACACS scheme to be referenced first. For RADIUS authorization, the RADIUS authorization scheme must be the same as the RADIUS authentication scheme. Otherwise, it does not take effect.
2. 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, limiting the authorization protocols that can be used for access.
3. Determine whether to configure an authorization method for all access types or service types.

Follow these guidelines when you configure AAA authorization methods for an ISP domain:

- The authorization method specified with the **authorization default** command is for all types of users and has a priority lower than that for a specific access type.
- If you configure an authentication method and an authorization method that use RADIUS schemes for an ISP domain, the RADIUS scheme for authorization must be the same as that for authentication. If the RADIUS authorization configuration is invalid or RADIUS authorization fails, the RADIUS authentication also fails. Whenever RADIUS authorization fails, an error message is sent to the NAS, indicating that the server is not responding.
- If you specify the **radius-scheme** *radius-scheme-name* **local**, **hwtacacs-scheme** *hwtacacs-scheme-name* [**local** | **none**] option when you configure an authorization method, local authorization or no authorization is the backup method and is used only when the remote server is not available.
- If you specify only the **local** or **none** keyword in an authorization method configuration command, the switch has no backup authorization method and performs only local authorization or does not perform any authorization.

To configure AAA authorization methods for an ISP domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter ISP domain view.	**domain** *isp-name*	N/A
3. Specify the default authorization method for all types of users.	**authorization default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The authorization method is **local** for all types of users.

Step	Command	Remarks
4. Specify the command authorization method.	**authorization command** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local** | **none**] | **local** | **none** }	Optional. The default authorization method is used by default.
5. Specify the authorization method for LAN users.	**authorization lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local** | **none**] }	Optional. The default authorization method is used by default.
6. Specify the authorization method for login users.	**authorization login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The default authorization method is used by default.
7. Specify the authorization method for portal users.	**authorization portal** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The default authorization method is used by default.

Configuring AAA accounting methods for an ISP domain

In AAA, accounting is a separate process at the same level as authentication and authorization. This process sends accounting start/update/end requests to the specified accounting server. Accounting is optional.

AAA supports the following accounting methods:

- **No accounting** (**none**)—The system does not perform accounting for the users.
- **Local accounting** (**local**)—Local accounting is implemented on the NAS. It counts and controls the number of concurrent users who use the same local user account. It does not provide statistics for charging. The maximum number of concurrent users using the same local user account is set by the **access-limit** command in local user view.
- **Remote accounting** (**scheme**)—The NAS works with a RADIUS server or HWTACACS server for accounting. You can configure local or no accounting as the backup method, which is used when the remote server is not available.

By default, an ISP domain uses the local accounting method.

Before configuring accounting methods, complete the following tasks:

1. For RADIUS or HWTACACS accounting, configure the RADIUS or HWTACACS scheme to be referenced first. The local and none accounting methods do not require a scheme.
2. 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, limiting the accounting protocols that can be used for access.
3. Determine whether to configure an accounting method for all access types or service types.

Follow these guidelines when you configure AAA accounting methods for an ISP domain:

- If you configure the **accounting optional** command, the limit on the number of local user connections is not effective.
- The accounting method specified with the **accounting default** command is for all types of users and has a priority lower than that for a specific access type.

- If you specify the **radius-scheme** *radius-scheme-name* **local** or **hwtacacs-scheme** *hwtacacs-scheme-name* **local** option when you configure an accounting method, local accounting is the backup method and is used only when the remote server is not available.
- If you specify only the **local** or **none** keyword in an accounting method configuration command, the switch has no backup accounting method and performs only local accounting or does not perform any accounting.
- Accounting is not supported for FTP services.

To configure AAA accounting methods for an ISP domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter ISP domain view.	**domain** *isp-name*	N/A
3. Enable the accounting optional feature.	**accounting optional**	Optional. Disabled by default. With the accounting optional feature, a switch allows users to use network resources when no accounting server is available or communication with all accounting servers fails.
4. Specify the default accounting method for all types of users.	**accounting default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The default accounting method is **local** for all types of users.
5. Specify the command accounting method.	**accounting command hwtacacs-scheme** *hwtacacs-scheme-name*	Optional. The default accounting method is used by default.
6. Specify the accounting method for LAN users.	**accounting lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local** | **none**] }	Optional. The default accounting method is used by default.
7. Specify the accounting method for login users.	**accounting login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The default accounting method is used by default.
8. Specify the accounting method for portal users.	**accounting portal** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Optional. The default accounting method is used by default.

Tearing down user connections

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step		Command	Remarks
2.	Tear down AAA user connections.	**cut connection** { **access-type** { **dot1x** | **mac-authentication** | **portal** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* } [**slot** *slot-number*]	The command applies only to LAN and portal user connections.

Configuring a NAS ID-VLAN binding

The access locations of users can be identified by their access VLANs. In application scenarios where identifying the access locations of users is a must, configure NAS ID-VLAN bindings on the switch. Then, when a user gets online, the switch obtains the NAS ID by the access VLAN of the user and sends the NAS ID to the RADIUS server through the NAS-identifier attribute.

To configure a NAS ID-VLAN binding:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a NAS ID profile and enter NAS ID profile view.	**aaa nas-id profile** *profile-name*	You can apply a NAS ID profile to an interface enabled with portal. See "Configuring portal authentication."
3.	Configure a NAS ID-VLAN binding.	**nas-id** *nas-identifier* **bind vlan** *vlan-id*	By default, no NAS ID-VLAN binding exists.

Configuring a switch as a RADIUS server

RADIUS server functions configuration task list

Task	Remarks
Configuring a RADIUS user	Required
Specifying a RADIUS client	Required

Configuring a RADIUS user

This task is to create a RADIUS user and configure a set of attributes for the user on a switch that serves as the RADIUS server. The user attributes include the password, authorization attribute, expiration time, and user description. After completing this task, the specified RADIUS user can use the username and password for RADIUS authentication on the switch.

You can use the **authorization-attribute** command to specify an authorization ACL and authorized VLAN, which is assigned by the RADIUS server to the RADIUS client (the NAS) after the RADIUS user passes authentication. The NAS then uses the assigned ACL and VLAN to control user access. If the assigned ACL does not exist on the NAS, ACL assignment fails and the NAS forcibly logs out the RADIUS user. If the assigned VLAN does not exist on the NAS, the NAS creates the VLAN and adds the RADIUS user or the access port to the VLAN.

To configure a RADIUS user:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a RADIUS user and enter RADIUS server user view.	**radius-server user** *user-name*	No RADIUS user exists by default.
3. Configure a password for the RADIUS user.	**password** [**cipher** | **simple**] *password*	Optional. By default, no password is specified.
4. Configure the authorization attribute for the RADIUS user.	**authorization-attribute** { **acl** *acl-number* | **vlan** *vlan-id* } *	Optional. Not configured by default.
5. Set the expiration time for the RADIUS user.	**expiration-date** *time*	Optional. By default, no expiration time is set, and the system does not check users' expiration time.
6. Configure a description for the RADIUS user.	**description** *text*	Optional. Not configured by default.

Specifying a RADIUS client

This task is to specify the IP address of a client to be managed by the RADIUS server and configure the shared key. The RADIUS server processes only the RADIUS packets sent from the specified clients.

To specify a RADIUS client

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify a RADIUS client.	**radius-server client-ip** *ip-address* [**key** [**cipher** | **simple**] *string*]	No RADIUS client is specified by default.

NOTE:

- The IP address of a RADIUS client specified on the RADIUS server must be consistent with the source IP address of outgoing RADIUS packets configured on the RADIUS client.
- The shared key configured on the RADIUS server must be consistent with that configured on the RADIUS client.

Displaying and maintaining AAA

Task	Command	Remarks
Display the configuration information of ISP domains.	**display domain** [*isp-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Task	Command	Remarks
Display information about user connections.	**display connection** [**access-type** { **dot1x** | **mac-authentication** | **portal** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

AAA configuration examples

Unless otherwise noted, devices in the configuration examples are operating in non-FIPS mode.

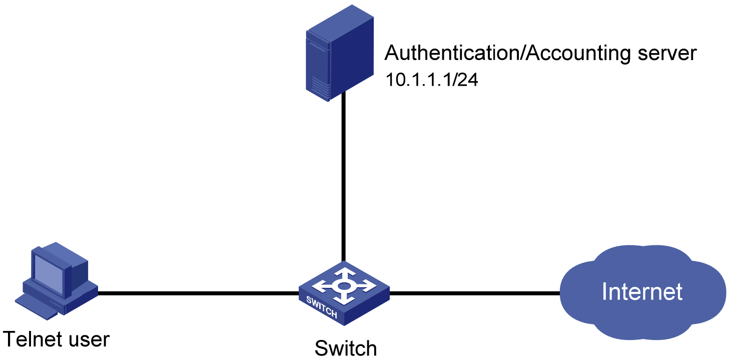
AAA for Telnet users by an HWTACACS server

Network requirements

As shown in Figure 10, configure the switch to use the HWTACACS server to provide authentication, authorization, and accounting services for Telnet users.

Set the shared keys for secure communication with the HWTACACS server to **expert**. Configure the switch to remove the domain name from a username before sending the username to the HWTACACS server.

Figure 10 Network diagram



Configuration procedure

1. Configure the switch:

   # Assign IP addresses to the interfaces. (Details not shown.)

   # Enable the Telnet server on the switch.

```
<Switch> system-view
[Switch] telnet server enable
```

   # Configure the switch to use AAA for Telnet users.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
[Switch-ui-vty0-4] quit
```

   # Create HWTACACS scheme **hwtac**.

```
[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 authentication, authorization, and accounting communication to **expert**.

```
[Switch-hwtacacs-hwtac] key authentication simple expert
[Switch-hwtacacs-hwtac] key authorization simple expert
[Switch-hwtacacs-hwtac] key accounting simple expert
```

# Configure the scheme to remove the domain name from a username before sending the username to the HWTACACS server.

```
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
```

# Configure the AAA methods for the domain.

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login hwtacacs-scheme hwtac
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting login hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
```

2. Verify the configuration:

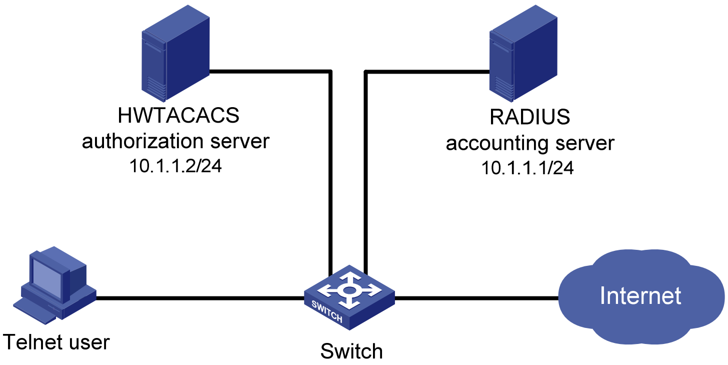
   Telnet to the switch as a user and enter the correct username and password. You pass authentication and log in to the switch. Issuing the **display connection** command on the switch, you can see information about the user connection.

AAA for Telnet users by separate servers

Network requirements

As shown in Figure 11, configure the switch to provide local authentication, HWTACACS authorization, and RADIUS accounting services for Telnet users. Set the shared keys for secure communication with the HWTACACS server and the RADIUS server to **expert**. Configure the switch to remove the domain name from a username before sending the username to the servers.

Figure 11 Network diagram



Configuration procedure

1. Configure the switch:

   # Assign IP addresses to interfaces. (Details not shown.)

   # Enable the Telnet server on the switch.

   ```
   <Switch> system-view
   [Switch] telnet server enable
   ```

   # Configure the switch to use AAA for Telnet users.

   ```
   [Switch] user-interface vty 0 4
   [Switch-ui-vty0-4] authentication-mode scheme
   [Switch-ui-vty0-4] quit
   ```

   # Configure the HWTACACS scheme.

   ```
   [Switch] hwtacacs scheme hwtac
   [Switch-hwtacacs-hwtac] primary authorization 10.1.1.2 49
   [Switch-hwtacacs-hwtac] key authorization expert
   [Switch-hwtacacs-hwtac] user-name-format without-domain
   [Switch-hwtacacs-hwtac] quit
   ```

   # Configure the RADIUS scheme.

   ```
   [Switch] radius scheme rd
   [Switch-radius-rd] primary accounting 10.1.1.1 1813
   [Switch-radius-rd] key accounting expert
   [Switch-radius-rd] server-type extended
   [Switch-radius-rd] user-name-format without-domain
   [Switch-radius-rd] quit
   ```

   # Create a local user named **hello**.

   ```
   [Switch] local-user hello
   [Switch-luser-hello] service-type telnet
   [Switch-luser-hello] password simple hello
   [Switch-luser-hello] quit
   ```

   # Configure the AAA methods for the ISP domain.

   ```
   [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
   ```

2. Verify the configuration:

   Telnet to the switch as a user and enter the username **hello@bbb** and the correct password. You pass authentication and log in to the switch. Issuing the **display connection** command on the switch, you can see information about the user connection.

Authentication/authorization for SSH/Telnet users by a RADIUS server

The configuration of authentication and authorization for SSH users is similar to that for Telnet users. The following example describes the configuration for SSH users.

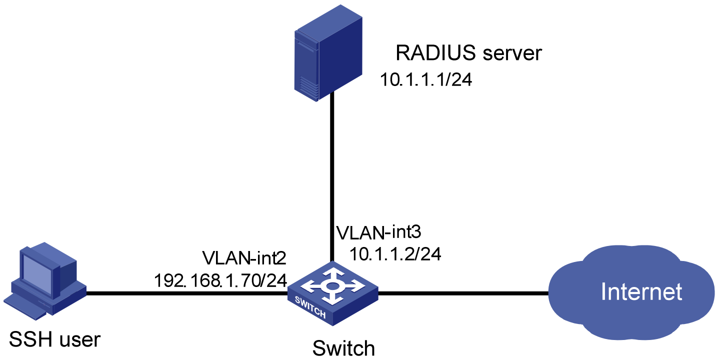
Network requirements

As shown in Figure 12, configure the switch to use the RADIUS server for SSH user authentication and authorization, and to include the domain name in a username sent to the RADIUS server.

Configure IMC to act as the RADIUS server, add an account with the username **hello@bbb** on the RADIUS server, and configure the RADIUS server to assign the privilege level of 3 to the user after the user passes authentication.

Set the shared keys for secure RADIUS communication to **expert**.

Figure 12 Network diagram



Configuring the RADIUS server

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

1. Add the switch to IMC as an access device:
   a. Log in to IMC, click the **Service** tab, and select **User Access Manager** > **Access Device** from the navigation tree.
   b. Click **Add**.
   c. Configure the following parameters:

      Set the shared key for secure authentication and accounting communication to **expert**.

      Specify the ports for authentication and accounting as 1812 and 1813, respectively.

      Select **Device Management Service** as the service type.

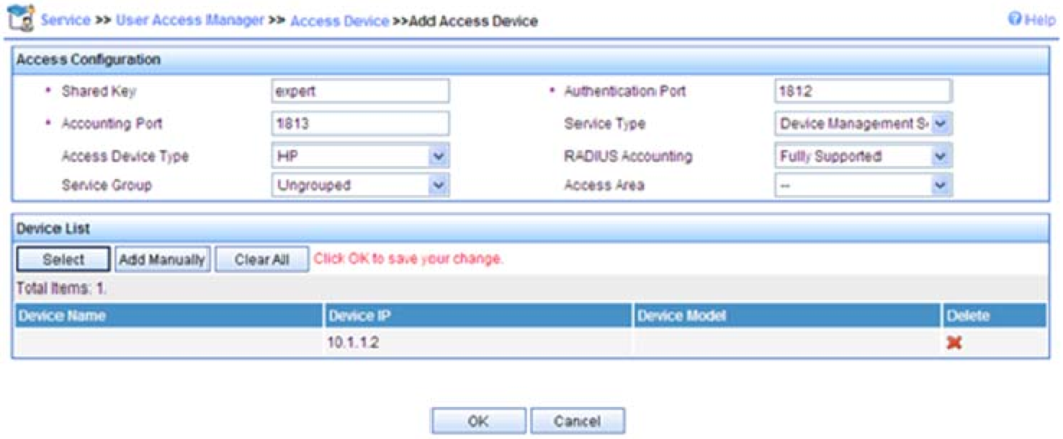
      Select **HP** as the access device type.

      Select the switch from the device list or manually add the switch with the IP address of 10.1.1.2.
   d. Click **OK**.

NOTE:

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, which is the IP address of the outbound interface by default, or otherwise the IP address specified with the **nas-ip** or **radius nas-ip** command on the switch.

Figure 13 Adding the switch to IMC as an access device


Service >> User Access Manager >> Access Device >>Add Access Device
Help

Access Configuration

* Shared Key	expert	* Authentication Port	1812
* Accounting Port	1813	Service Type	Device Management S
Access Device Type	HP	RADIUS Accounting	Fully Supported
Service Group	Ungrouped	Access Area	--

Device List

Select
Add Manually
Clear All

Click OK to save your change.

Total Items: 1.

Device Name	Device IP	Device Model	Delete
	10.1.1.2		✖

2. Add a user for device management:
   a. Click the **User** tab, and select **Device Management User** from the navigation tree.
   b. Click **Add**.
   c. Configure the following parameters:

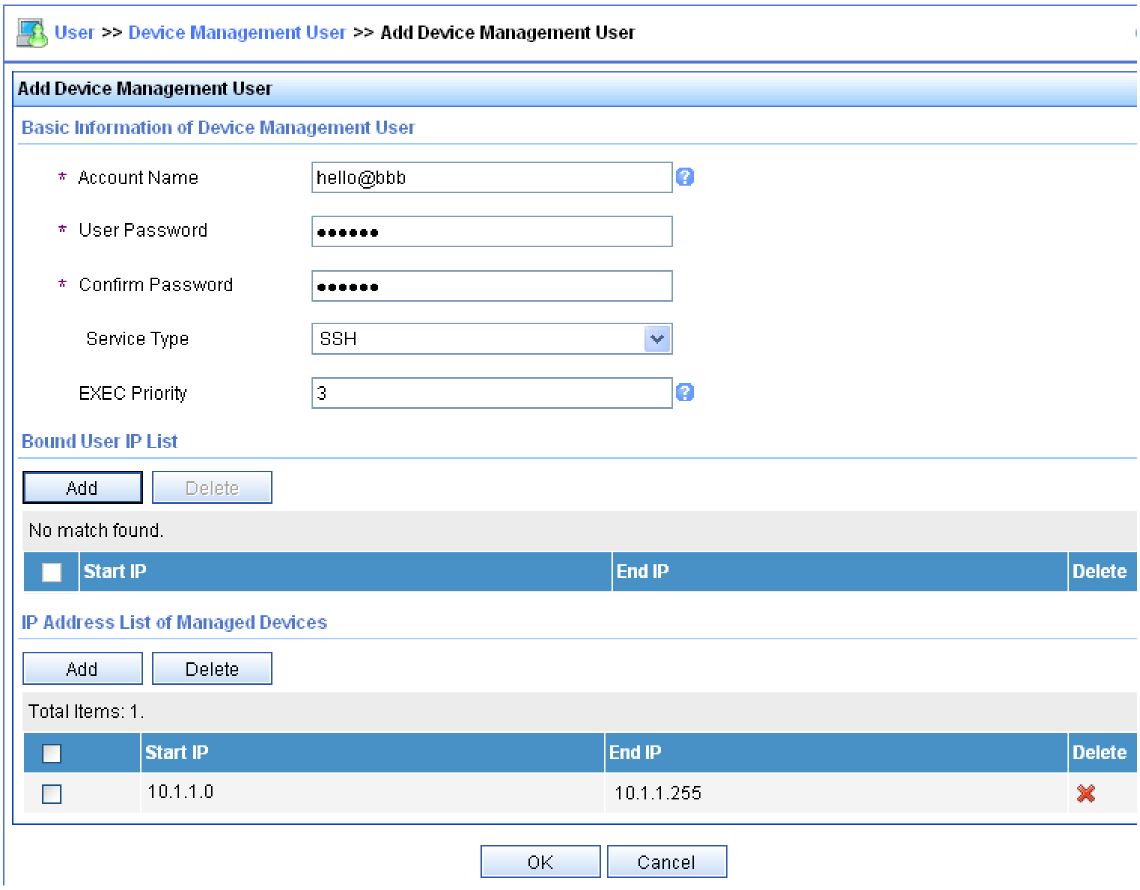
      Enter **hello@bbb** as the username and set the password.

      Select **SSH** as the service type.

      Set the EXEC privilege level to 3. This value identifies the privilege level of the SSH user after login and defaults to 0.

      Specify the IP address range of the hosts to be managed as 10.1.1.0 through 10.1.1.255.
   d. Click **OK**.

Figure 14 Adding an account for device management



User >> Device Management User >> Add Device Management User

Add Device Management User

Basic Information of Device Management User

* Account Name	hello@bbb
* User Password	••••••
* Confirm Password	••••••
Service Type	SSH
EXEC Priority	3

Bound User IP List

No match found.

□	Start IP	End IP	Delete

IP Address List of Managed Devices

Total Items: 1.

□	Start IP	End IP	Delete
□	10.1.1.0	10.1.1.255	✗

Configuring 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 access the server.

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

# Generate RSA and DSA key pairs and enable the SSH server.

```
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```

# Configure the switch to use AAA for SSH users.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

# Configure the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

# Create RADIUS scheme **rad**.

```
[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 authentication communication to **expert**.

```
[Switch-radius-rad] key authentication expert
```

# Configure the scheme to include the domain names in usernames to be sent to the RADIUS server.

```
[Switch-radius-rad] user-name-format with-domain
```

# Specify the service type for the RADIUS server, which must be **extended** when the RADIUS server runs on IMC.

```
[Switch-radius-rad] server-type extended
[Switch-radius-rad] quit
```

# Configure the AAA methods for the domain.

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] quit
```

Verifying the configuration

After you complete the configuration, the SSH user should be able to use the configured account to access the user interface of the switch and can access the demands of level 0 through level 3. .

# Use the **display connection** command to view the connection information on the switch.

```
[Switch] display connection
Index=1   ,Username=hello@bbb
IP=192.168.1.58
IPv6=N/A
 Total 1 connection(s) matched.
```

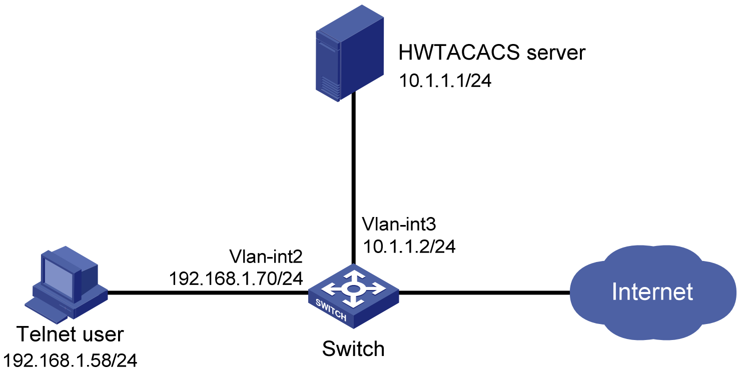
Level switching authentication for Telnet users by an HWTACACS server

Network requirements

As shown in Figure 15, configure the switch to:

- Use local authentication for the Telnet user and assign the privilege level of 0 to the user after the user passes authentication.
- Use the HWTACACS server for level switching authentication of the Telnet user, and use local authentication as the backup.

Figure 15 Network diagram



Configuration considerations

1. Configure the switch to use AAA, particularly, local authentication for Telnet users:
   - Create ISP domain **bbb** and configure it to use local authentication for Telnet users.
   - Create a local user account, configure the password, and assign the user privilege level.
2. On the switch, configure the authentication method for user privilege level switching:
   - Specify to use HWTACACS authentication and, if HWTACACS authentication is not available, use local authentication for user level switching authentication.
   - Configure HWTACACS scheme **hwtac** and assign an IP address to the HWTACACS server. Set the shared keys for message exchange and specify that usernames sent to the HWTACACS server carry no domain name. Configure the domain to use the HWTACACS scheme **hwtac** for user privilege level switching authentication.
   - Configure the password for local privilege level switching authentication.
3. On the HWTACACS server, add the username and password for user privilege level switching authentication.

Configuration procedure

1. Configure the switch:

   # Configure the IP address of VLAN-interface 2, through which the Telnet 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
   ```

   # Enable the switch to provide Telnet service.

   ```
   [Switch] telnet server enable
   ```

   # Configure the switch to use AAA for Telnet users.

   ```
   [Switch] user-interface vty 0 4
   [Switch-ui-vty0-4] authentication-mode scheme
   [Switch-ui-vty0-4] quit
   ```

# Use HWTACACS authentication for user level switching authentication and, if HWTACACS authentication is not available, use local authentication.

```
[Switch] super authentication-mode scheme local
```

# Create an HWTACACS scheme named **hwtac**.

```
[Switch] hwtacacs scheme hwtac
```

# Specify the IP address for the primary authentication server as 10.1.1.1 and the port for authentication as 49.

```
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
```

# Set the shared key for secure authentication communication to **expert**.

```
[Switch-hwtacacs-hwtac] key authentication simple expert
```

# Configure the scheme to remove the domain name from a username before sending the username to the HWTACACS server.

```
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
```

# Create ISP domain **bbb**.

```
[Switch] domain bbb
```

# Configure the ISP domain to use local authentication for Telnet users.

```
[Switch-isp-bbb] authentication login local
```

# Configure to use HWTACACS scheme **hwtac** for privilege level switching authentication.

```
[Switch-isp-bbb] authentication super hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
```

# Create a local Telnet user named **test**.

```
[Switch] local-user test
[Switch-luser-test] service-type telnet
[Switch-luser-test] password simple aabbcc
```

# Configure the user level of the Telnet user to 0 after user login.

```
[Switch-luser-test] authorization-attribute level 0
[Switch-luser-test] quit
```

# Configure the password for local privilege level switching authentication to **654321**.

```
[Switch] super password simple 654321
[Switch] quit
```

2. Configure the HWTACACS server:

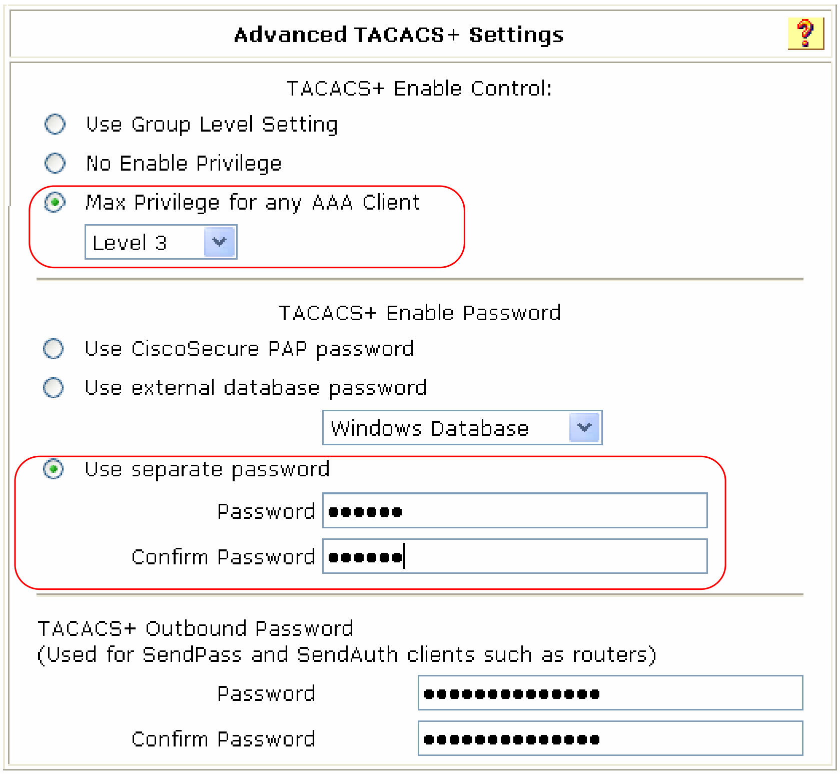
NOTE:

The HWTACACS server in this example runs ACSv4.0.

Add a user named **test** on the HWTACACS server and configure advanced attributes for the user as shown in Figure 16:

- Select **Max Privilege for any AAA Client** and set the privilege level to level 3. This setting requires the user to enter the password when switching to level 1, level 2, or level 3.
- Select **Use separate password** and specify the password as **enabpass**.

Figure 16 Configuring advanced attributes for the Telnet user



Advanced TACACS+ Settings

TACACS+ Enable Control:

○ Use Group Level Setting

○ No Enable Privilege

● Max Privilege for any AAA Client

Level 3

TACACS+ Enable Password

○ Use CiscoSecure PAP password

○ Use external database password

Windows Database

● Use separate password

Password ●●●●●●

Confirm Password ●●●●●●

TACACS+ Outbound Password
(Used for SendPass and SendAuth clients such as routers)

Password ●●●●●●●●●●●●●●

Confirm Password ●●●●●●●●●●●●●●

3. Verify the configuration:

   After you complete the configuration, the Telnet user should be able to telnet to the switch and use username **test@bbb** and password **aabbcc** to enter the user interface of the switch, and access all level 0 commands.

```
<Switch> telnet 192.168.1.70
Trying 192.168.1.70 ...
Press CTRL+K to abort
Connected to 192.168.1.70 ...
******************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                   *
******************************************************************************

Login authentication

Username:test@bbb
Password:
<Switch> ?
User view commands:
  display  Display current system information
  ping     Ping function
  quit     Exit from current command view
  ssh2     Establish a secure shell client connection
  super    Set the current user priority level
  telnet   Establish one TELNET connection
  tracert  Trace route function
```

When switching to user privilege level 3, the Telnet user only needs to enter password **enabpass** as prompted.

```
<Switch> super 3
 Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

If the HWTACACS server is not available, the Telnet user needs to enter password **654321** as prompted for local authentication.

```
<Switch> super 3
 Password: ← Enter the password for HWTACACS privilege level switch authentication
 Error: Invalid configuration or no response from the authentication server.
 Info: Change authentication mode to local.
 Password: ← Enter the password for local privilege level switch authentication
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

RADIUS authentication and authorization for Telnet users by a switch

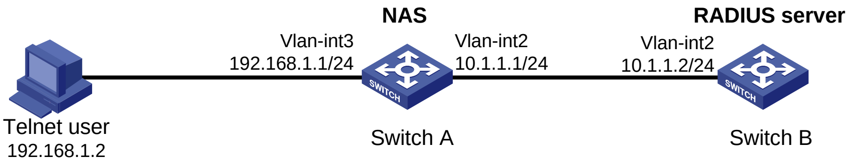
Network requirements

As shown in Figure 17, configure Switch B to act as a RADIUS server to provide authentication and authorization for the Telnet user on port 1645.

Configure Switch A to use the RADIUS server for Telnet user authentication and authorization, and to remove the domain name in a username sent to the server.

Set the shared keys for secure communication between the NAS and the RADIUS server to **abc**.

Figure 17 Network diagram



Configuration procedure

1. Assign an IP address to each interface as shown in Figure 17. (Details not shown.)
2. Configure the NAS:

   # Enable the Telnet server on Switch A.

   ```
   <SwitchA> system-view
   [SwitchA] telnet server enable
   ```

   # Configure Switch A to use AAA for Telnet users.

   ```
   [SwitchA] user-interface vty 0 4
   [SwitchA-ui-vty0-4] authentication-mode scheme
   ```

```
[SwitchA-ui-vty0-4] quit
```

# Create RADIUS scheme **rad**.

```
[SwitchA] radius scheme rad
```

# Specify the IP address for the primary authentication server as 10.1.1.2, the port for authentication as 1645, and the shared key for secure authentication communication as **abc**.

```
[SwitchA-radius-rad] primary authentication 10.1.1.2 1645 key abc
```

# Configure the scheme to remove the domain name from a username before sending the username to the RADIUS server.

```
[SwitchA-radius-rad] user-name-format without-domain
```

# Set the source IP address for RADIUS packets as 10.1.1.1.

```
[SwitchA-radius-rad] nas-ip 10.1.1.1
[SwitchA-radius-rad] quit
```

# Create ISP domain **bbb**.

```
[SwitchA] domain bbb
```

# Specify the authentication method for Telnet users as **rad**.

```
[SwitchA-isp-bbb] authentication login radius-scheme rad
```

# Specify the authorization method for Telnet users as **rad**.

```
[SwitchA-isp-bbb] authorization login radius-scheme rad
```

# Specify the accounting method for Telnet users as **none**.

```
[SwitchA-isp-bbb] accounting login none
```

# Configure the RADIUS server type as **standard**. When a switch is configured to serve as a RADIUS server, the server type must be set to **standard**.

```
[SwitchA-isp-bbb] server-type standard
[SwitchA-isp-bbb] quit
```

# Configure **bbb** as the default ISP domain. Then, if a user enters a username without any ISP domain at login, the authentication and accounting methods of the default domain is used for the user.

```
[SwitchA] domain default enable bbb
```

3. Configure the RADIUS server:

# Create RADIUS user **aaa** and enter its view.

```
<SwitchB> system-view
[SwitchB] radius-server user aaa
```

# Configure plaintext password **aabbcc** for user **aaa**.

```
[SwitchB-rdsuser-aaa] password simple aabbcc
[SwitchB-rdsuser-aaa] quit
```

# Specify the IP address of the RADIUS client as 10.1.1.1 and the plaintext shared key as **abc**.

```
[SwitchB] radius-server client-ip 10.1.1.1 key simple abc
```

4. Verify the configuration:

After entering username **aaa@bbb** or **aaa** and password **aabbcc**, user **aaa** can telnet to Switch A. Use the **display connection** command to view the connection information on Switch A.

```
<SwitchA> display connection

Index=1   ,Username=aaa@bbb
IP=192.168.1.2
IPv6=N/A
```

```
Total 1 connection(s) matched.
```

Troubleshooting AAA

Troubleshooting RADIUS

Symptom 1

User authentication/authorization always fails.

Analysis

1. A communication failure exists between the NAS and the RADIUS server.
2. The username is not in the format of *userid@isp-name* or the ISP domain for the user authentication is not correctly configured on the NAS.
3. The user is not configured on the RADIUS server.
4. The password entered by the user is incorrect.
5. The RADIUS server and the NAS are configured with different shared key.

Solution

Check that:

1. The NAS and the RADIUS server can ping each other.
2. The username is in the *userid@isp-name* format and the ISP domain for the user authentication is correctly configured on the NAS.
3. The user is configured on the RADIUS server.
4. The correct password is entered.
5. The same shared key is configured on both the RADIUS server and the NAS.

Symptom 2

RADIUS packets cannot reach the RADIUS server.

Analysis

1. The NAS and the RADIUS server cannot communicate with each other.
2. The NAS is not configured with the IP address of the RADIUS server.
3. The UDP ports for authentication/authorization and accounting are not correct.
4. The port numbers of the RADIUS server for authentication, authorization and accounting are being used by other applications.

Solution

Check that:

1. The communication links between the NAS and the RADIUS server work well at both physical and link layers.
2. The IP address of the RADIUS server is correctly configured on the NAS.
3. UDP ports for authentication/authorization/accounting configured on the NAS are the same as those configured on the RADIUS server.
4. The port numbers of the RADIUS server for authentication, authorization and accounting are available.

Symptom 3

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

Analysis

1. The accounting port number is not correct.
2. Configuration of the authentication/authorization server and the accounting server are not correct on the NAS. For example, one server is configured on the NAS to provide all the services of authentication/authorization and accounting, but in fact the services are provided by different servers.

Solution

Check that:

1. The accounting port number is correctly set.
2. The authentication/authorization server and the accounting server are correctly configured on the NAS.

Troubleshooting HWTACACS

Similar to RADIUS troubleshooting. See "Troubleshooting RADIUS."

802.1X overview

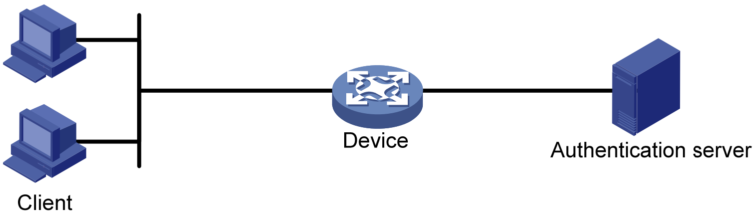
802.1X is a port-based network access control protocol initially proposed by the IEEE 802 LAN/WAN committee for securing wireless LANs (WLANs), and it has also been widely used on Ethernet networks for access control.

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. It comprises three entities: the client (the supplicant), the network access device (the authenticator), and the authentication server.

Figure 18 802.1X architecture



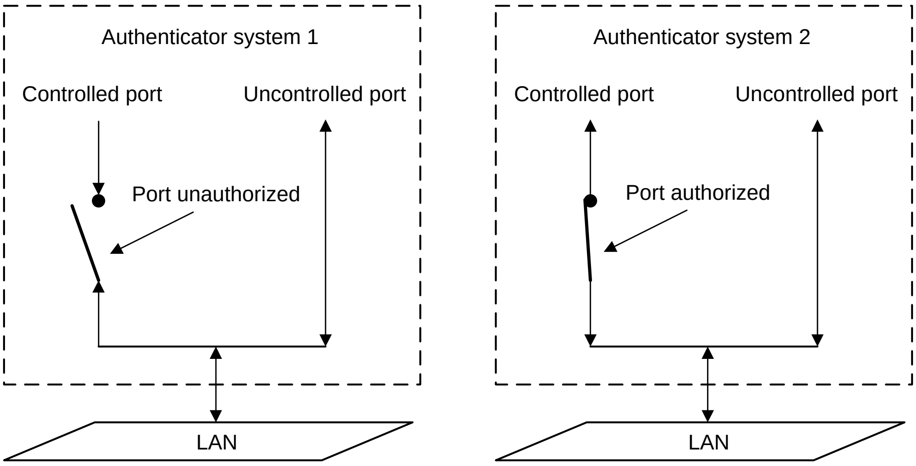
- **The client**—A user terminal seeking access to the LAN. It must have 802.1X software to authenticate to the network access device.
- **The network access device**—Authenticates the client to control access to the LAN. In a typical 802.1X environment, the network access device uses an authentication server to perform authentication.
- **The authentication server**—Provides authentication services for the network access device. It authenticates 802.1X clients by using the data sent from the network access device, and returns the authentication results for the network access device to make access decisions. The authentication server is typically a Remote Authentication Dial-in User Service (RADIUS) server. In a small LAN, you can also use the network access device as the authentication server.

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.

- **Controlled port**—Allows incoming and outgoing traffic to pass through when it is in the authorized state, and denies incoming and outgoing traffic when it is in the unauthorized state, as shown in Figure 19. The controlled port is set in the authorized state if the client has passed authentication, and in the unauthorized state, if the client has failed authentication.
- **Uncontrolled port**—Is always open to receive and transmit EAPOL frames.

Figure 19 Authorization state of a controlled port



In the unauthorized state, a controlled port controls traffic in one of the following ways:

- Performs bidirectional traffic control to deny traffic to and from the client.
- Performs unidirectional traffic control to deny traffic from the client.

The HP 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 network access device, and the authentication server. EAP is an authentication framework that uses the client/server model. It 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 network access device over a wired or wireless LAN. Between the network access device and the authentication server, 802.1X delivers authentication information in one of the following methods:

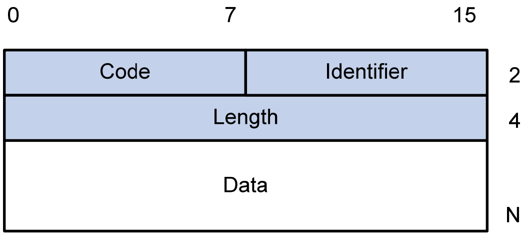
- Encapsulates EAP packets in RADIUS by using EAP over RADIUS (EAPOR), as described in "EAP relay."
- Extracts authentication information from the EAP packets and encapsulates the information in standard RADIUS packets, as described in "EAP termination."

Packet formats

EAP packet format

Figure 20 shows the EAP packet format.

Figure 20 EAP packet format

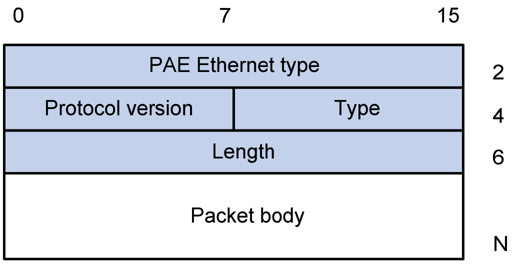


- **Code**—Type of the EAP packet. Options include Request (1), Response (2), Success (3), or Failure (4).
- **Identifier**—Used for matching Responses with Requests.
- **Length**—Length (in bytes) of the EAP packet. The EAP packet length is the sum of the Code, Identifier, Length, and Data fields.
- **Data**—Content of the EAP packet. This field appears only in a Request or Response EAP packet. The field comprises 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 21 shows the EAPOL packet format.

Figure 21 EAPOL packet format



- **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 5 lists the types of EAPOL packets supported by HP implementation of 802.1X.

Table 5 EAPOL packet types

Value	Type	Description
0x00	EAP-Packet	The client and the network access device uses EAP-Packets to transport authentication information.
0x01	EAPOL-Start	The client sends an EAPOL-Start message to initiate 802.1X authentication to the network access device.

Value	Type	Description
0x02	EAPOL-Logoff	The client sends an EAPOL-Logoff message to tell the network access device that it is logging off.

- **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.

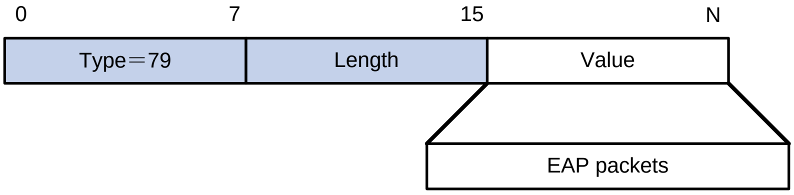
EAP over RADIUS

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 22. 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.

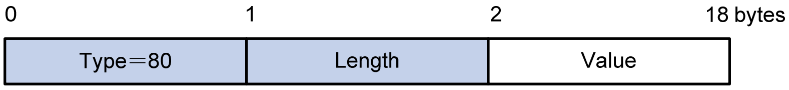
Figure 22 EAP-Message attribute format



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 than the Message-Authenticator attribute value. The Message-Authenticator prevents EAP authentication packets from being tampered with during EAP authentication.

Figure 23 Message-Authenticator attribute format



Initiating 802.1X authentication

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, the HP iNode 802.1X client for example, that can send broadcast EAPOL-Start packets.

Access device as the initiator

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

The access device supports the following modes:

- **Multicast trigger mode**—The access device multicasts Identity EAP-Request packets periodically (every 30 seconds by default) to initiate 802.1X authentication.
- **Unicast trigger mode**—Upon receiving a frame with the source MAC address not in the MAC address table, the access device sends an Identity EAP-Request packet out of the receiving port to the unknown MAC address. It retransmits the packet if no response has been received within a certain time interval.

802.1X authentication procedures

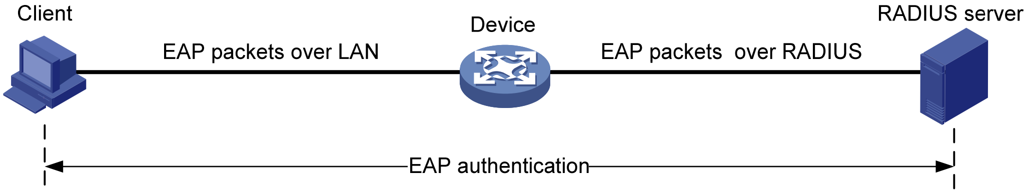
802.1X authentication has two approaches: EAP relay and EAP termination. You choose either mode depending on the support of the RADIUS server for EAP packets and EAP authentication methods.

- 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 24.

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

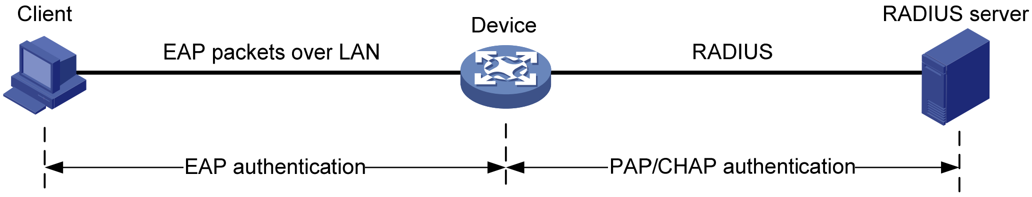
Figure 24 EAP relay



- EAP termination mode

  In EAP termination mode, the network access device terminates the EAP packets received from the client, encapsulates the client authentication information in standard RADIUS packets, and uses (Password Authentication Protocol) PAP or (Password Authentication Protocol) CHAP to authenticate to the RADIUS server, as shown in Figure 25.

Figure 25 EAP termination



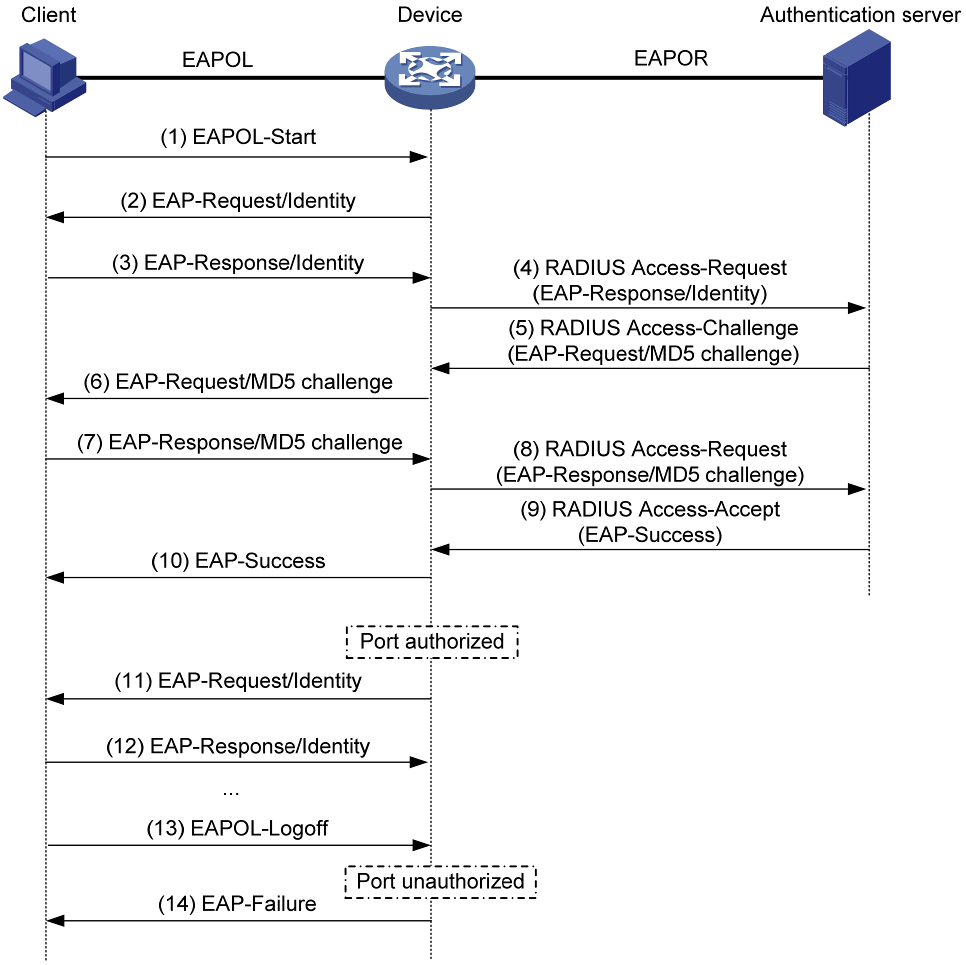
A comparison of EAP relay and EAP termination

Packet exchange method	Benefits	Limitations
EAP relay	• Supports various EAP authentication methods. • The configuration and processing is simple on the network 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 MD5-Challenge EAP authentication and the "username + password" EAP authentication initiated by an HP iNode 802.1X client. • The processing is complex on the network access device.

EAP relay

Figure 26 shows the basic 802.1X authentication procedure in EAP relay mode, assuming that EAP-MD5 is used.

Figure 26 802.1X authentication procedure in EAP relay mode


Client
Device
Authentication server
EAPOL
EAPOR
(1) EAPOL-Start
(2) EAP-Request/Identity
(3) EAP-Response/Identity
(4) RADIUS Access-Request (EAP-Response/Identity)
(5) RADIUS Access-Challenge (EAP-Request/MD5 challenge)
(6) EAP-Request/MD5 challenge
(7) EAP-Response/MD5 challenge
(8) RADIUS Access-Request (EAP-Response/MD5 challenge)
(9) RADIUS Access-Accept (EAP-Success)
(10) EAP-Success
Port authorized
(11) EAP-Request/Identity
(12) EAP-Response/Identity
...
(13) EAPOL-Logoff
Port unauthorized
(14) EAP-Failure

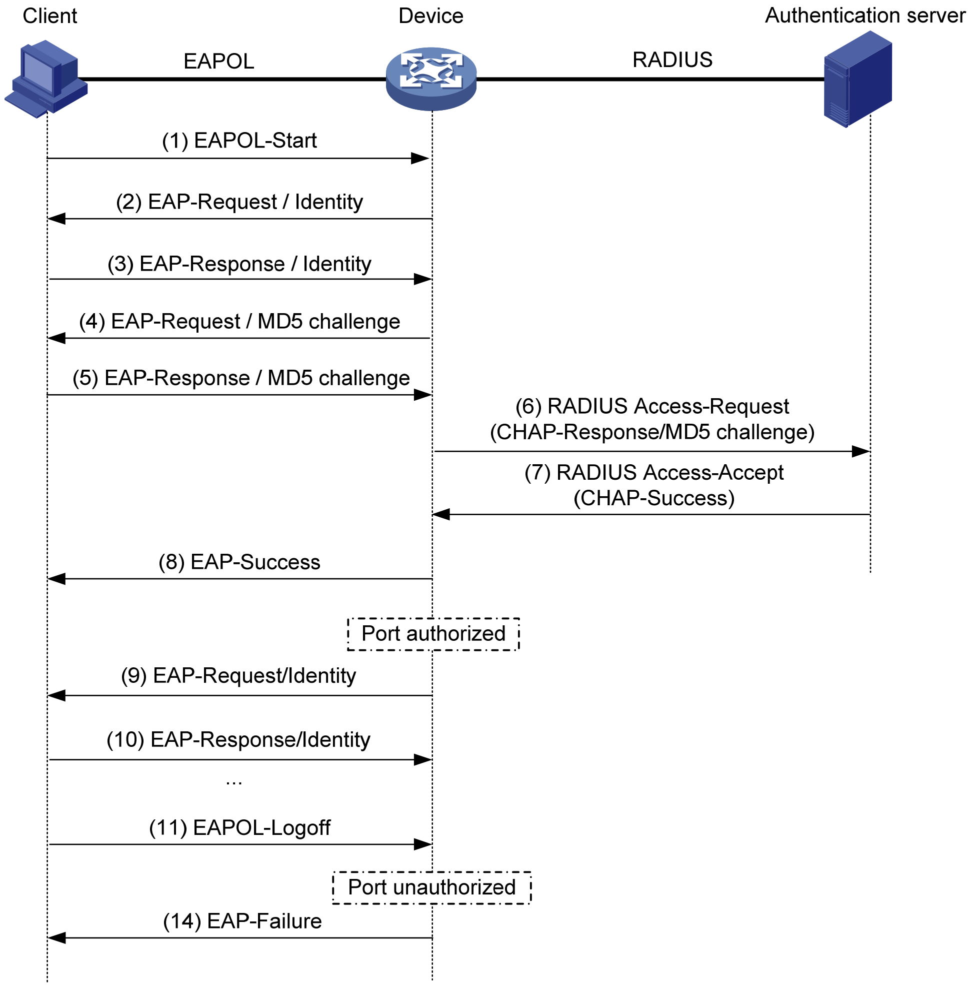
1. When a user launches the 802.1X client software and enters a registered username and password, the 802.1X client software sends an EAPOL-Start packet to the network access device.
2. The network access device responds with an Identity EAP-Request packet to ask for the client username.
3. In response to the Identity EAP-Request packet, the client sends the username in an Identity EAP-Response packet to the network access device.
4. The network 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, and sends the challenge in a RADIUS Access-Challenge packet to the network access device.
6. The network access device relays the EAP-Request/MD5 Challenge packet in a RADIUS Access-Request 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 network access device.
8. The network 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 one it generated at step 5. If the two are identical, the authentication server considers the client valid and sends a RADIUS Access-Accept packet to the network access device.
10. Upon receiving the RADIUS Access-Accept packet, the network access device sends an EAP-Success packet to the client, and sets the controlled port in the authorized state so the client can access the network.
11. After the client comes online, the network 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 certain number of consecutive handshake attempts (two by default), the network access device logs off the client. This handshake mechanism enables timely release of the network resources used by 802.1X users that have abnormally gone offline.
13. The client can also send an EAPOL-Logoff packet to ask the network access device for a logoff. Then
14. In response to the EAPOL-Logoff packet, the network access device changes the status of the controlled port from authorized to unauthorized and sends an EAP-Failure packet to the client.

EAP termination

Figure 27 shows the basic 802.1X authentication procedure in EAP termination mode, assuming that CHAP authentication is used.

Figure 27 802.1X authentication procedure in EAP termination mode



In EAP termination mode, it is the network access device rather than the authentication server generates an MD5 challenge for password encryption (see Step 4). The network 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 HP 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. Port security is beyond the scope of this chapter. It is described in "Port security configuration."

HP implementation of 802.1X

Access control methods

HP 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.

Using 802.1X authentication with other features

VLAN assignment

The device can work with a RADIUS server to assign VLANs to 802.1X users. The device accepts untagged VLANs that are assigned through the RFC 3580-compliant Tunnel attributes and tagged VLANs that are assigned through the RFC 4675-compliant Egress-VLANID or Egress-VLAN-Name attribute.

NOTE:

- Access ports do not support RFC 4675-compliant assignment of VLANs.
- Trunk and hybrid ports support RFC 4675-compliant assignment of only tagged VLANs.

Table 6 and Table 7 describes how the device handles VLANs assigned through a RADIUS server

Table 6 VLAN assignment in port-based access control mode

Link type	VLAN assignment
Access port	Sets the VLAN ID assigned through the Tunnel attributes as the PVID on the port. All subsequent users can access the network, regardless of their VLANs. When the authenticated user logs off, the previous PVID restores, and all users attached to the port cannot access the network.
Trunk/hybrid port	• Sets the VLAN ID assigned through the Tunnel attributes as the PVID on the port. • Assigns the port to the VLANs assigned through the Egress-VLANID or Egress-VLAN-Name attribute, and sets the VLANs as tagged VLANs.

Table 7 VLAN assignment in MAC-based access control mode

Link type	VLAN assignment
Access	Sets the VLAN ID assigned through the Tunnel attributes to the first authenticated user as the PVID on the port. If a different VLAN is assigned to a subsequent user, the user cannot pass the authentication. To avoid the authentication failure of subsequent users, be sure to assign the same VLAN to all 802.1X users that are attached to an access port.
Trunk	• Sets the VLAN assigned through the Tunnel attributes as the PVID on the port. • Assigns the port to VLANs assigned through the Egress-VLANID or Egress-VLAN-Name attribute.
Hybrid	• If MAC-based VLAN is disabled, the VLAN assignment actions are the same as on a trunk port. • If MAC-based VLAN is enabled, the device does the following actions: ○ Maps the user's MAC address to the VLAN assigned through the Tunnel attributes, and sets the VLAN as an untagged VLAN. ○ Maps the user's MAC address to the VLAN assigned through the Egress-VLANID or Egress-VLAN-Name attribute, and sets the VLAN as a tagged VLAN. When a user logs off, the MAC-to-VLAN mapping for the user is removed. If MAC-based VLAN is enabled, the device does not replace the PVID on the port with a server assigned VLAN, regardless of whether the assignment is through Tunnel attributes or the Egress-VLANID attribute.

On a periodic online user re-authentication enabled port, if a user has been online before you enable the MAC-based VLAN function, the device does not create a MAC-to-VLAN mapping for the user unless the user passes re-authentication and the VLAN for the user has changed.

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

VLAN group assignment

Use VLAN group assignment to balance users across several VLANs.

VLAN group assignment allows the authentication server to assign a VLAN group to the access device for an 802.1X user. From this VLAN group, the device picks a VLAN for the 802.1X user in the following order:

1. Selects the VLAN that has the fewest number of online 802.1X users.

   If a port performs port-based access control, all 802.1X users attached to the port are counted as one user.

2. If two VLANs have the same number of 802.1X users, the device selects the VLAN with the lower ID.

Guest VLAN

You can configure a guest VLAN on a port to accommodate users that have not performed 802.1X authentication, so they can access a limited set of network resources, such as a software server, to download anti-virus software and system patches. After a user in the guest VLAN passes 802.1X authentication, it is removed from the guest VLAN and can access authorized network resources. The way that the network access device handles VLANs on the port differs by 802.1X access control mode.

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

1. On a port that performs port-based access control

Authentication status	VLAN manipulation
No 802.1X user has performed authentication within 90 seconds after 802.1X is enabled	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, 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	• Assigns the VLAN specified for the user to the port as the PVID, and removes the port from the 802.1X guest VLAN. After the user logs off, the user configured PVID restores. • If the authentication server assigns no VLAN, the user-configured PVID applies. The user and all subsequent 802.1X users are assigned to the user-configured port VLAN. After the user logs off, the PVID remains unchanged.

2. On a port that performs MAC-based access control

To use the 802.1X guest VLAN function on a port that performs MAC-based access control, make sure that the port is a hybrid port, and enable MAC-based VLAN on the port.

Authentication status	VLAN manipulation
A user has not passed 802.1X authentication yet	Creates a mapping between the MAC address of the user and the 802.1X guest VLAN. The user can access resources in the guest VLAN.
A user in the 802.1X guest VLAN fails 802.1X authentication	If an 802.1X Auth-Fail VLAN is available, re-maps 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	Re-maps the MAC address of the user to the VLAN specified for the user. If the authentication server assigns no VLAN, re-maps the MAC address of the user to the initial PVID on the port.

NOTE:

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

Auth-Fail VLAN

You can configure an Auth-Fail VLAN to accommodate users that have failed 802.1X authentication because of the failure to comply with the organization security strategy, such as using a wrong password.

Users in the Auth-Fail VLAN can access a limited set of network resources, such as a software server, to download anti-virus software and system patches.

The Auth-Fail VLAN does not accommodate 802.1X users that have failed authentication for authentication timeouts or network connection problems. The way that the network access device handles VLANs on the port differs by 802.1X access control mode.

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

1. On a port that performs port-based access control

Authentication status	VLAN manipulation
A user fails 802.1X authentication	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.
A user in the Auth-Fail VLAN fails 802.1X re-authentication	The Auth-Fail VLAN is still the PVID on the port, and all 802.1X users on this port are in this VLAN.
A user passes 802.1X authentication	• Assigns the VLAN specified for the user to the port as the PVID, and removes the port from the Auth-Fail VLAN. After the user logs off, the user-configured PVID restores. • If the authentication server assigns no VLAN, the initial PVID applies. The user and all subsequent 802.1X users are assigned to the user-configured PVID. After the user logs off, the PVID remains unchanged.

2. On a port that performs MAC-based access control

To perform the 802.1X Auth-Fail VLAN function on a port that performs MAC-based access control, you must make sure that the port is a hybrid port, and enable MAC-based VLAN on the port.

Authentication status	VLAN manipulation
A user fails 802.1X authentication	Re-maps the MAC address of the user to the Auth-Fail VLAN. The user can access only resources in the Auth-Fail VLAN.
A user in the Auth-Fail VLAN fails 802.1X re-authentication	The user is still in the Auth-Fail VLAN.
A user in the Auth-Fail VLAN passes 802.1X authentication	Re-maps the MAC address of the user to the server-assigned VLAN. If the authentication server assigns no VLAN, re-maps the MAC address of the user to the initial PVID on the port.

NOTE:

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

Critical VLAN

You configure an 802.1X critical VLAN on a port to accommodate 802.1X users that fail authentication because none of the RADIUS authentication servers in their ISP domain is reachable (active). Users in the critical VLAN can access a limit set of network resources depending on your 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."

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

The way that the network access device handles VLANs on an 802.1X-enabled port differs by 802.1X access control mode.

1. On a port that performs port-based access control

Authentication status	VLAN manipulation
A user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.	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 critical VLAN.
A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable.	The critical VLAN is still the PVID of the port, and all 802.1X users on this port are in this VLAN.
A user in the 802.1X critical VLAN fails authentication for any other reason than server unreachable.	If an Auth-Fail VLAN has been configured, the PVID of the port changes to Auth-Fail VLAN ID, and all 802.1X users on this port are moved to the Auth-Fail VLAN.
A user in the critical VLAN passes 802.1X authentication.	• Assigns the VLAN specified for the user to the port as the PVID, and removes the port from the critical VLAN. After the user logs off, the default or user-configured PVID restores. • If the authentication server assigns no VLAN, the default or user-configured PVID applies. The user and all subsequent 802.1X users are assigned to this port VLAN. After the user logs off, this PVID remains unchanged.
A user in the 802.1X guest VLAN or the Auth-Fail VLAN fails authentication because all the RADIUS servers is reachable.	The PVID of the port remains unchanged. All 802.1X users on this port can access only resources in the guest VLAN or the Auth-Fail VLAN.

2. On a port that performs MAC-based access control

To perform the 802.1X critical VLAN function on a port that performs MAC-based access control, you must make sure that the port is a hybrid port, and enable MAC-based VLAN on the port.

Authentication status	VLAN manipulation
A user that has not been assigned to any VLAN fails 802.1X authentication because all the RADIUS servers are unreachable.	Maps the MAC address of the user to the critical VLAN. The user can access only resources in the critical VLAN.

Authentication status	VLAN manipulation
A user in the 802.1X critical VLAN fails authentication because all the RADIUS servers are unreachable.	The user is still in the critical VLAN.
A user in the critical VLAN fails 802.1X authentication for any other reason than server unreachable.	If an Auth-Fail VLAN has been configured, re-maps the MAC address of the user to the Auth-Fail VLAN ID.
A user in the critical VLAN passes 802.1X authentication.	Re-maps the MAC address of the user to the server-assigned VLAN. If the authentication server assigns no VLAN, re-maps the MAC address of the user to the default or user-configured PVID on the port.
A user in the 802.1X guest VLAN or the Auth-Fail VLAN fails authentication because all the RADIUS server are unreachable.	The user remains in the 802.1X VLAN or the Auth-Fail VLAN.
A user in the MAC authentication guest VLAN fails 802.1X authentication because all the 802.1X authentication server are unreachable.	The user is removed from the MAC authentication VLAN and mapped to the 802.1X critical VLAN.

NOTE:

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

Any of the following RADIUS authentication server changes in the ISP domain for 802.1X users on a port can cause the users to be removed from the critical VLAN:

- An authentication server is added to the ISP domain and the server is reachable.
- A response from a RADIUS authentication server is received.
- The RADIUS server probing function detects that a RADIUS authentication server is reachable.

You can use the **dot1x critical recovery-action reinitialize** command to configure the port to trigger 802.1X re-authentication when the port or an 802.1X user on the port is removed from the critical VLAN.

- If MAC-based access control is used, the port sends a unicast Identity EAP/Request to the 802.1X user to trigger authentication.
- If port-based access control is used, the port sends a multicast Identity EAP/Request to the 802.1X users to trigger authentication.

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, either the local access device or a RADIUS server, assigns the ACL to the port to filter the traffic from this user. In either case, you must configure the ACL on the access device. You can change ACL rules while the user is online.

Configuration prerequisites

- 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**.

802.1X configuration task list

Task	Remarks
Enabling 802.1X	Required
Enabling EAP relay or EAP termination	Optional
Setting the port authorization state	Optional
Specifying an access control method	Optional
Setting the maximum number of concurrent 802.1X users on a port	Optional
Setting the maximum number of authentication request attempts	Optional
Setting the 802.1X authentication timeout timers	Optional
Configuring the online user handshake function	Optional
Configuring the authentication trigger function	Optional
Specifying a mandatory authentication domain on a port	Optional
Configuring the quiet timer	Optional
Enabling the periodic online user re-authentication function	Optional
Configuring a port to send EAPOL frames untagged	Optional
Setting the maximum number of 802.1X authentication attempts for MAC authentication users	Optional
Configuring a VLAN group	Optional
Configuring an 802.1X guest VLAN	Optional
Configuring an 802.1X Auth-Fail VLAN	Optional
Configuring an 802.1X critical VLAN	Optional
Specifying supported domain name delimiters	Optional

Enabling 802.1X

Configuration guidelines

- If the PVID of a port is a voice VLAN, the 802.1X function cannot take effect on the port. For more information about voice VLANs, see *Layer 2—LAN Switching Configuration Guide*.
- 802.1X is mutually exclusive with link aggregation configuration on a port.
- Do not use the BPDU drop feature on an 802.1X-enabled port. The BPDU drop feature discards 802.1X packets arrived on the port.

Configuration procedure

To enable 802.1X on a port:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable 802.1X globally.	**dot1x**	By default, 802.1X is disabled globally.
3.	Enable 802.1X on a port.	- In system view: **dot1x interface** *interface-list* - In Ethernet interface view: a. **interface** *interface-type interface-number* b. **dot1x**	Use either method. By default, 802.1X is disabled on a port.

Enabling EAP relay or EAP termination

When you configure EAP relay or EAP termination, consider the following factors:

- The support of the RADIUS server for EAP packets
- The authentication methods supported by the 802.1X client and the RADIUS server

If the client is using only MD5-Challenge EAP authentication or the "username + password" EAP authentication initiated by an HP iNode 802.1X client, you can use both EAP termination and EAP relay. To use EAP-TL, PEAP, or any other EAP authentication methods, you must use EAP relay. When you make your decision, see "A comparison of 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:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure EAP relay or EAP termination.	**dot1x authentication-method** { **chap** | **eap** | **pap** }	Optional. By default, the network access device performs EAP termination and uses CHAP to communicate with the RADIUS server. Specify the **eap** keyword to enable EAP termination. Specify the **chap** or **pap** keyword to enable CHAP-enabled or PAP-enabled EAP relay.

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. 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 the unauthorized state to allow only EAPOL packets to pass, and 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.

You can set authorization state for one port in Ethernet interface view, or for multiple ports in system view. If different authorization state is set for a port in system view and Ethernet interface view, the one set later takes effect.

To set the authorization state of a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the port authorization state.	• In system view: **dot1x port-control** { **authorized-force** | **auto** | **unauthorized-force** } [**interface** *interface-list*] • In Ethernet interface view: a. **interface** *interface-type interface-number* b. **dot1x port-control** { **authorized-force** | **auto** | **unauthorized-force** }	Optional. Use either method. By default, **auto** applies.

Specifying an access control method

You can specify an access control method for one port in Ethernet interface view, or for multiple ports in system view. If different access control methods are specified for a port in system view and Ethernet interface view, the one specified later takes effect.

To use both 802.1X and portal authentication on a port, you must specify MAC-based access control. For information about portal authentication, see "Configuring portal authentication."

To specify the access control method:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Specify an access control method.	- In system view: **dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*] - In Ethernet interface view: **a.** **interface** *interface-type interface-number* **b.** **dot1x port-method** { **macbased** | **portbased** }	Optional. Use either method. By default, MAC-based access control applies.

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

You can set the maximum number of concurrent 802.1X users for ports individually in Ethernet interface view or in bulk in system view. If different settings are configured for a port in both views, the setting configured later takes effect.

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

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the maximum number of concurrent 802.1X users on a port.	- In system view: **dot1x max-user** *user-number* [**interface** *interface-list*] - In Ethernet interface view: **a.** **interface** *interface-type interface-number* **b.** **dot1x max-user** *user-number* [**interface** *interface-list*]	Optional. Use either method. The default maximum number of concurrent 802.1X users on a port is 256.

Setting the maximum number of authentication request attempts

The network access device retransmits an authentication request if it receives no response to the request it has sent to the client within a period of time (specified by using the **dot1x timer tx-period** *tx-period-value* command or the **dot1x timer supp-timeout** *supp-timeout-value* command). The network access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.

To set the maximum number of authentication request attempts:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Set the maximum number of attempts for sending an authentication request.	**dot1x retry** *max-retry-value*	Optional. The default setting is 2.

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.

You can set the client timeout timer to a high value in a low-performance network, and adjust the server timeout timer to adapt to the performance of different authentication servers. In most cases, the default settings are sufficient.

To set the 802.1X authentication timeout timers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the client timeout timer.	**dot1x timer supp-timeout** *supp-timeout-value*	Optional. The default is 30 seconds.
3. Set the server timeout timer.	**dot1x timer server-timeout** *server-timeout-value*	Optional. The default is 100 seconds.

Configuring the online user handshake function

The online user handshake function checks the connectivity status of online 802.1X users. The network access device sends handshake messages to online users at the interval specified by the **dot1x timer handshake-period** command. If no response is received from an online user after the maximum number of handshake attempts (set by the **dot1x retry** command) has been made, the network access device sets the user in the offline state.

If iNode clients are deployed, you can also enable the online handshake security function to check for 802.1X users that use illegal client software to bypass security inspection such as proxy detection and dual network interface cards (NICs) detection. This function checks the authentication information in client handshake messages. If a user fails the authentication, the network access device logs the user off.

Configuration guidelines

Follow these guidelines when you configure the online user handshake function:

- To use the online handshake security function, make sure the online user handshake function is enabled. HP recommends that you use the iNode client software and IMC server to guarantee the normal operation of the online user handshake security function.

- If the network has 802.1X clients that cannot exchange handshake packets with the network access device, disable the online user handshake function to prevent their connections from being inappropriately torn down.

Configuration procedure

To configure the online user handshake function:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the handshake timer.	**dot1x timer handshake-period** *handshake-period-value*	Optional. The default is 15 seconds.
3. Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Enable the online handshake function.	**dot1x handshake**	Optional. By default, the function is enabled.
5. Enable the online handshake security function.	**dot1x handshake secure**	Optional. By default, the function is disabled.

Configuring the authentication trigger function

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

This function provides the following types of authentication trigger:

- **Multicast trigger**—Periodically multicasts Identity EAP-Request packets out of a port to detect 802.1X clients and trigger authentication.
- **Unicast trigger**—Enables the network device to initiate 802.1X authentication when it receives a data frame from an unknown source MAC address. The device sends a unicast Identity EAP/Request packet to the unknown source MAC address, and retransmits the packet if it has received no response within a period of time. This process continues until the maximum number of request attempts set with the **dot1x retry** command (see "Setting the maximum number of authentication request attempts") is reached.

The identity request timeout timer sets both the identity request interval for the multicast trigger and the identity request timeout interval for the unicast trigger.

Configuration guidelines

Follow these guidelines when you configure the authentication trigger function:

- 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 function on a port:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the username request timeout timer.	**dot1x timer tx-period** *tx-period-value*	Optional. The default is 30 seconds.
3.	Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4.	Enable an authentication trigger.	**dot1x** { **multicast-trigger** | **unicast-trigger** }	Required if you want to enable the unicast trigger. By default, the multicast trigger is enabled, and the unicast trigger is disabled.

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:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Specify a mandatory 802.1X authentication domain on the port.	**dot1x mandatory-domain** *domain-name*	By default, no mandatory 802.1X authentication domain is specified.

Configuring the quiet timer

The quiet timer enables the network 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 set the quiet timer to a high value in a vulnerable network or a low value for quicker authentication response.

To configure the quiet timer:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the quiet timer.	**dot1x quiet-period**	By default, the timer is disabled.
3.	Set the quiet timer.	**dot1x timer quiet-period** *quiet-period-value*	Optional. The default is 60 seconds.

Enabling the periodic online user re-authentication function

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

Configuration guidelines

- The periodic online user re-authentication timer can also be set by the authentication server in the session-timeout attribute. The server-assigned timer overrides the timer setting on the access device, and enables periodic online user re-authentication, even if the function is not configured. Support for the server assignment of re-authentication timer and the re-authentication timer configuration on the server vary with servers.
- The VLAN assignment status must be consistent before and after re-authentication. If the authentication server has assigned a VLAN before re-authentication, it must also assign a VLAN at re-authentication. If the authentication server has assigned no VLAN before re-authentication, it must not assign one at re-authentication. Violation of either rule can cause the user to be logged off. The VLANs assigned to an online user before and after re-authentication can be the same or different.
- If no critical VLAN is configured, RADIUS server unreachable can cause an online user being re-authenticated to be logged off. If a critical VLAN is configured, the user remains online and in the original VLAN.

Configuration procedure

To enable the periodic online user re-authentication function:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the periodic re-authentication timer.	**dot1x timer reauth-period** *reauth-period-value*	Optional. The default is 3600 seconds.
3.	Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4.	Enable periodic online user re-authentication.	**dot1x re-authenticate**	By default, the function is disabled.

Configuring a port to send EAPOL frames untagged

EAPOL frames exchanged between the 802.1X client and the network access device must not contain VLAN tags. If any 802.1X user attached to a port is assigned a tagged VLAN, you must enable the port to send EAPOL frames untagged to 802.1X clients.

To configure a port to send EAPOL packets untagged to 802.1X clients:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the port to send 802.1X EAPOL frames untagged.	**dot1x eapol untag**	By default, whether the port sends EAPOL packets with a VLAN tag depends on the VLAN settings on the port.

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

If both MAC authentication and 802.1X authentication are enabled on a port, the device allows an authenticated MAC authentication user to initiate an 802.1X authentication. If the user passes 802.1X authentication, the user goes online as an 802.1X user. If the user fails 802.1X authentication, the user can retry authentication until the maximum number of authentication attempts is reached.

To set the maximum number of 802.1X authentication attempts for MAC authentication users:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Set the maximum number of 802.1X authentication attempts for MAC authentication users.	**dot1x attempts max-fail** *unsuccessful-attempts*	By default, an authenticated MAC authentication user can retry 802.1X authentication until the maximum number of authentication attempts configured on the 802.1X client is reached.

Configuring a VLAN group

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Create a VLAN group and enter its view.	**vlan-group** *group-name*	By default, no VLAN group exists.
3. Add VLANs to the group.	**vlan-list** *vlan-list*	By default, a VLAN group does not contain VLANs. You can repeat this step to add VLANs.

Configuring an 802.1X guest VLAN

Configuration guidelines

Follow these guidelines when you configure an 802.1X guest VLAN:

- 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, so the port can correctly process incoming VLAN tagged traffic.
- With 802.1X authentication, 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.
- If 802.1X clients in your network cannot trigger an immediate DHCP-assigned IP address renewal in response to a VLAN change, the 802.1X users cannot access authorized network resources immediately after an 802.1X authentication is complete. As a solution, remind the 802.1X users to release their IP addresses or repair their network connections for a DHCP reassignment after 802.1X authentication is complete. The HP iNode client does not have this problem.
- Use Table 8 when configuring multiple security features on a port.

Table 8 Relationships of the 802.1X guest VLAN and other security features

Feature	Relationship description	Reference
MAC authentication guest VLAN on a port that performs MAC-based access control	Only the 802.1X guest VLAN take effect. A user that fails MAC authentication will not be assigned to the MAC authentication guest VLAN.	See "Configuring MAC authentication"
802.1X Auth-Fail VLAN on a port that performs MAC-based access control	The 802.1X Auth-Fail VLAN has a higher priority	See "Using 802.1X authentication with other features"
Port intrusion protection on a port that performs MAC-based access control	The 802.1X guest VLAN function has higher priority than the block MAC action but lower priority than the shut down port action of the port intrusion protection feature.	See "Configuring port security"

Configuration prerequisites

- Create the VLAN to be specified as the 802.1X guest VLAN.
- If the 802.1X-enabled port performs port-based access control, enable 802.1X multicast trigger (**dot1x multicast-trigger**).

- If the 802.1X-enabled port performs MAC-based access control, configure the port as a hybrid port, enable MAC-based VLAN on the port, and assign the port to the 802.1X guest VLAN as an untagged member. For more information about the MAC-based VLAN function, see *Layer 2—LAN Switching Configuration Guide*.

Configuration procedure

To configure an 802.1X guest VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure an 802.1X guest VLAN for one or more ports.	• In system view: **dot1x guest-vlan** *guest-vlan-id* [**interface** *interface-list*] • In Ethernet interface view: a. **interface** *interface-type interface-number* b. **dot1x guest-vlan** *guest-vlan-id*	Use either method. By default, no 802.1X guest VLAN is configured on any port.

Configuring an 802.1X Auth-Fail VLAN

Configuration guidelines

Follow these guidelines when configuring an 802.1X Auth-Fail VLAN:

- Assign different IDs to the voice VLAN, the port VLAN, and the 802.1X Auth-Fail VLAN on a port, so 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.
- If 802.1X clients in your network cannot trigger an immediate DHCP-assigned IP address renewal in response to a VLAN change, the 802.1X users cannot access authorized network resources immediately after an 802.1X authentication is complete. As a solution, remind the 802.1X users to release their IP addresses or repair their network connections for a DHCP reassignment after 802.1X authentication is complete. The HP iNode client does not have this problem.
- Use Table 9 when configuring multiple security features on a port.

Table 9 Relationships of the 802.1X Auth-Fail VLAN with other features

Feature	Relationship description	Reference
MAC authentication guest VLAN on a port that performs MAC-based access control	The 802.1X Auth-Fail VLAN has a high priority.	See "Configuring MAC authentication"
Port intrusion protection on a port that performs MAC-based access control	The 802.1X Auth-Fail VLAN function has higher priority than the block MAC action but lower priority than the shut down port action of the port intrusion protection feature.	See "Configuring port security"

Configuration prerequisites

- Create the VLAN to be specified as the 802.1X Auth-Fail VLAN.
- If the 802.1X-enabled port performs port-based access control, enable 802.1X multicast trigger (**dot1x multicast-trigger**).
- If the 802.1X-enabled port performs MAC-based access control, configure the port as a hybrid port, enable MAC-based VLAN on the port, and assign the port to the Auth-Fail VLAN as an untagged member. For more information about the MAC-based VLAN function, see *Layer 2—LAN Switching Configuration Guide*.

Configuration procedure

To configure an Auth-Fail VLAN:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure the Auth-Fail VLAN on the port.	**dot1x auth-fail vlan** *authfail-vlan-id*	By default, no Auth-Fail VLAN is configured.

Configuring an 802.1X critical VLAN

Configuration guidelines

- Assign different IDs to the voice VLAN, the port VLAN, and the 802.1X critical VLAN on a port, so 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.
- If 802.1X clients in your network cannot trigger an immediate DHCP-assigned IP address renewal in response to a VLAN change, the 802.1X users cannot access authorized network resources immediately after an 802.1X authentication is complete. As a solution, remind the 802.1X users to release their IP addresses or repair their network connections for a DHCP reassignment after 802.1X authentication is complete. The HP iNode client does not have this problem.

Configuration prerequisites

- Create the VLAN to be specified as a critical VLAN.
- If the 802.1X-enabled port performs port-based access control, enable 802.1X multicast trigger (**dot1x multicast-trigger**).
- If the 802.1X-enabled port performs MAC-based access control, configure the port as a hybrid port, enable MAC-based VLAN on the port, and assign the port to the Auth-Fail VLAN as an untagged member. For more information about the MAC-based VLAN function, see *Layer 2—LAN Switching Configuration Guide*.

Configuration procedure

To configure an 802.1X critical VLAN:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure an 802.1X critical VLAN on the port.	**dot1x critical vlan** *vlan-id*	By default, no critical VLAN is configured.
4.	Configure the port to trigger 802.1X authentication on detection of a reachable authentication server for users in the critical VLAN.	**dot1x critical recovery-action reinitialize**	Optional. By default, when a reachable RADIUS server is detected, the system removes the port or 802.1X users from the critical VLAN without triggering authentication.

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 that use other domain name delimiters.

The configurable delimiters include the at sign (@), back slash (\), and forward slash (/).

If an 802.1X username string contains multiple configured delimiters, the leftmost delimiter is the domain name delimiter. For example, if you configure @, /, and \ as delimiters, the domain name delimiter for the username string 123/22\@abc is the forward slash (/).

If a username string contains none of the delimiters, the access device authenticates the user in the mandatory or default ISP domain. The access selects a domain delimiter from the delimiter set in this order: @, /, and \.

Follow the steps to specify a set of domain name delimiters:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Specify a set of domain name delimiters for 802.1X users.	**dot1x domain-delimiter** *string*	Optional. By default, only the at sign (@) delimiter is supported.

NOTE:

If you configure the access device to include the domain name in the username sent to the RADIUS server, make sure the domain delimiter in the username can be recognized by the RADIUS server. For username format configuration, see the **user-name-format** command in *Security Command Reference*.

Displaying and maintaining 802.1X

Task	Command	Remarks
Display 802.1X session information, statistics, or configuration information of specified or all ports.	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear 802.1X statistics.	**reset dot1x statistics** [**interface** *interface-list*]	Available in user view

802.1X authentication configuration example

Network requirements

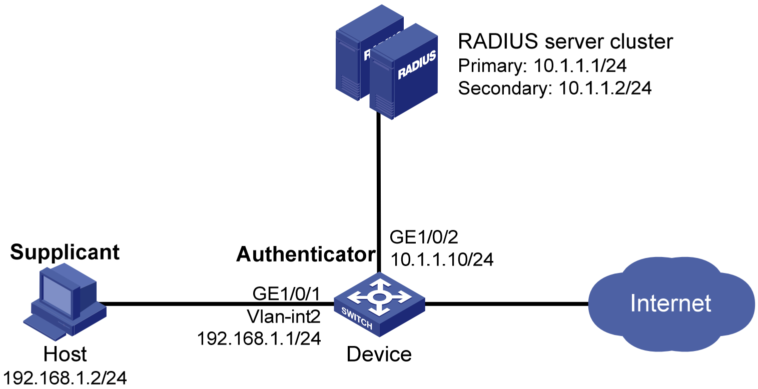
As shown in Figure 28, the access device performs 802.1X authentication for users that connect to port GigabitEthernet 1/0/1. Implement MAC-based access control on the port, so the logoff of one user does not affect other online 802.1X users.

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. If RADIUS accounting fails, the access device logs the user off.

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 **aabbcc.net**, which accommodates up to 30 users.

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

Figure 28 Network diagram



Configuration procedure

1. Configure the 802.1X client. If HP 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. For information about the RADIUS commands used on the access device in this example, see *Security Command Reference*. (Details not shown.)
3. Assign an IP address to 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 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 server.)

```
<Device> system-view
[Device] local-user localuser
[Device-luser-localuser] service-type lan-access
[Device-luser-localuser] password simple localpass
```

# Configure the idle cut function to log off any online user that has been idled for 20 minutes.

```
[Device-luser-localuser] authorization-attribute idle-cut 20
[Device-luser-localuser] quit
```

5. Configure a RADIUS scheme:

# Create the RADIUS scheme **radius1** and enter its 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 name
```

# Specify the shared key between the access device and the accounting server.

```
[Device-radius-radius1] key accounting money
```

# Exclude the ISP domain name from the username 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 **aabbcc.net** and enter its view.

```
[Device] domain aabbcc.net
```

# Apply the RADIUS scheme **radius1** to the ISP domain, and specify local authentication as the secondary authentication method.

```
[Device-isp-aabbcc.net] authentication lan-access radius-scheme radius1 local
[Device-isp-aabbcc.net] authorization lan-access radius-scheme radius1 local
[Device-isp-aabbcc.net] accounting lan-access radius-scheme radius1 local
```

# Set the maximum number of concurrent users in the domain to 30.

```
[Device-isp-aabbcc.net] access-limit enable 30
```

# Configure the idle cut function to log off any online domain user that has been idle for 20 minutes.

```
[Device-isp-aabbcc.net] idle-cut enable 20
[Device-isp-aabbcc.net] quit
```

# Specify **aabbcc.net** as the default ISP domain. If a user does not provide any ISP domain name, it is assigned to the default ISP domain.

```
[Device] domain default enable aabbcc.net
```

7. Configure 802.1X:

   # Enable 802.1X globally.

   ```
   [Device] dot1x
   ```

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

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

   # Enable MAC-based access control on the port. (Optional. MAC-based access control is the default setting.)

   ```
   [Device] dot1x port-method macbased interface gigabitethernet 1/0/1
   ```

Verifying the configuration

Use the **display dot1x interface gigabitethernet 1/0/1** command to verify the 802.1X configuration. After an 802.1X user passes RADIUS authentication, you can use the **display connection** command to view the user connection information. If the user fails RADIUS authentication, local authentication is performed.

802.1X with guest VLAN and VLAN assignment configuration example

Network requirements

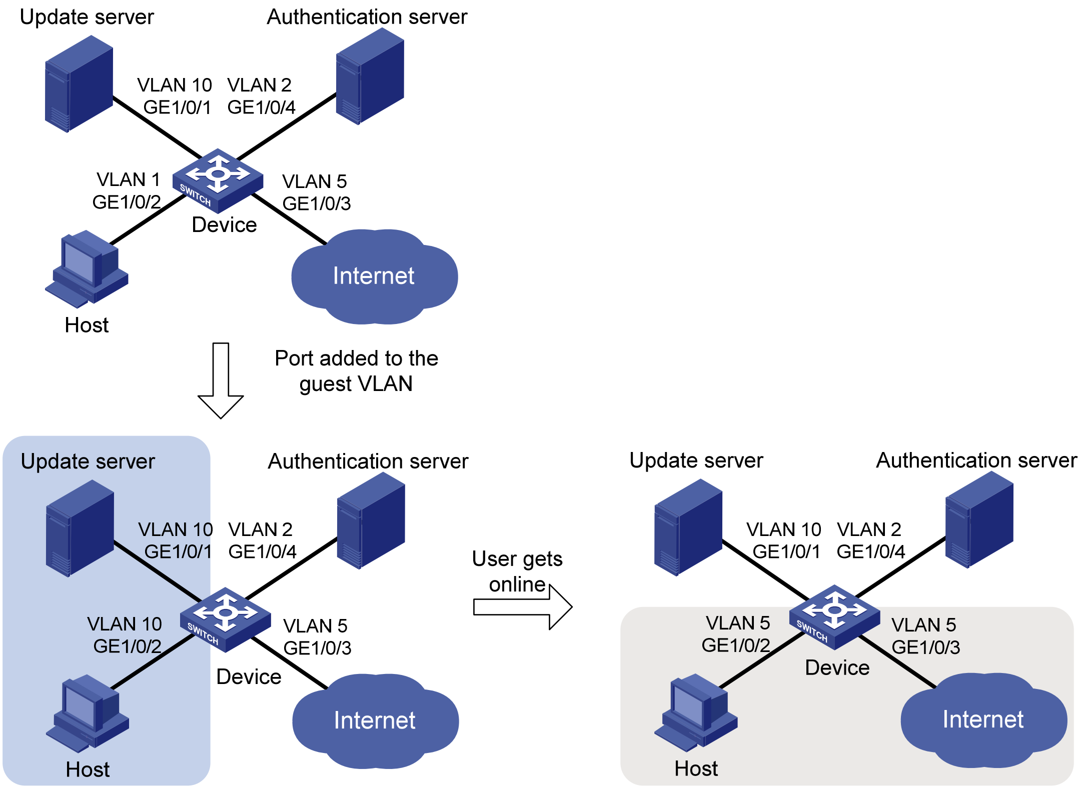
As shown in Figure 29:

- A host is connected to port GigabitEthernet 1/0/2 of the device and must pass 802.1X authentication to access the Internet. GigabitEthernet 1/0/2 is in VLAN 1.
- GigabitEthernet 1/0/2 implements port-based access control.
- GigabitEthernet 1/0/3 is in VLAN 5 and is for accessing the Internet.
- The authentication server runs RADIUS and is in VLAN 2.
- The update server in VLAN 10 is for client software download and upgrade.

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 its 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 network access device assigns the host to VLAN 5 where GigabitEthernet 1/0/3 is. The host can access the Internet.

Figure 29 Network diagram



Configuration procedure

The following configuration procedure covers most AAA/RADIUS configuration commands on the device. The configuration on the 802.1X client and RADIUS server are not shown. For more information about AAA/RADIUS configuration commands, see *Security Command Reference*.

1. Make sure the 802.1X client can update its IP address after the access port is assigned to the guest VLAN or a server-assigned VLAN. (Details not shown.)
2. Configure the RADIUS server to provide authentication, authorization, and accounting services. Configure user accounts and server-assigned VLAN, VLAN 5 in this example. (Details not shown.)
3. Create VLANs, and assign ports to the VLANs.

```
<Device> system-view
[Device] vlan 1
[Device-vlan1] port gigabitethernet 1/0/2
[Device-vlan1] quit
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/4
[Device-vlan2] quit
[Device] vlan 5
[Device-vlan5] port gigabitethernet 1/0/3
[Device-vlan5] quit
```

4. Configure a RADIUS scheme:

   # Configure RADIUS scheme **2000** and enter its view.

```
<Device> system-view
[Device] radius scheme 2000
```

   # Specify primary and secondary authentication and accounting servers. Set the shared key to **abc** for authentication and accounting packets.

```
[Device-radius-2000] primary authentication 10.11.1.1 1812
[Device-radius-2000] primary accounting 10.11.1.1 1813
[Device-radius-2000] key authentication abc
[Device-radius-2000] key accounting abc
```

   # Exclude the ISP domain name from the username 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 its view.

```
[Device] domaim 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:

   # Enable 802.1X globally.

```
[Device] dot1x
```

   # Enable 802.1X for 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**. This step is optional. By default, the port is in auto mode.

```
[Device-GigabitEthernet1/0/2] dot1x port-control auto
[Device-GigabitEthernet1/0/2] quit
```

   # Set VLAN 10 as the 802.1X guest VLAN for port GigabitEthernet 1/0/2.

```
[Device] dot1x guest-vlan 10 interface gigabitethernet 1/0/2
```

Verifying the configuration

Use the **display dot1x interface gigabitethernet 1/0/2** command to verify the 802.1X guest VLAN configuration on GigabitEthernet 1/0/2. If no user passes authentication on the port within a specific period of time, use the **display vlan 10** command to verify whether GigabitEthernet 1/0/2 is assigned to VLAN 10.

After a user passes authentication, you can use the **display interface gigabitethernet 1/0/2** command to verity that port GigabitEthernet 1/0/2 has been added to VLAN 5.

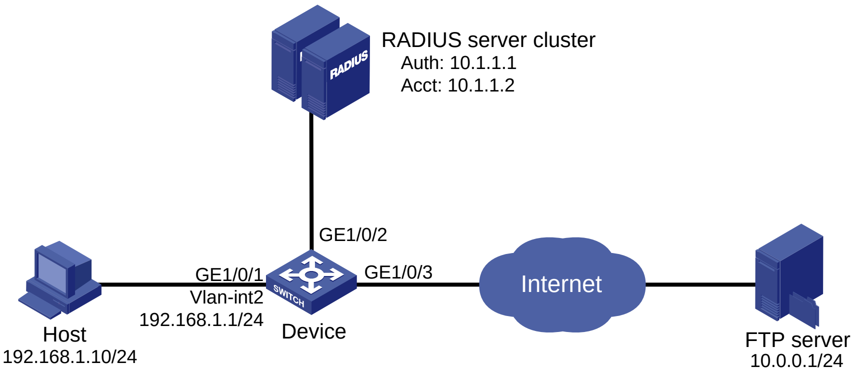
802.1X with ACL assignment configuration example

Network requirements

As shown in Figure 30, the host at 192.168.1.10 connects to port GigabitEthernet 1/0/1 of the network access device.

Perform 802.1X authentication on the port. 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. Assign an ACL to GigabitEthernet 1/0/1 to deny the access of 802.1X users to the FTP server at 10.0.0.1/24 on weekdays during business hours from 8:00 to 18:00.

Figure 30 Network diagram



Configuration procedure

The following configuration procedure provides the major AAA and RADIUS configuration on the access device. The configuration procedures on the 802.1X client and RADIUS server are beyond the scope of this configuration example. For information about AAA and RADIUS configuration commands, see *Security Command Reference*.

1. Configure 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 a server-assigned VLAN. (Details not shown.)
2. Configure the RADIUS servers, user accounts, and authorization ACL, ACL 3000 in this example. (Details not shown.)
3. Configure the access device:

   # Assign IP addresses to interfaces. (Details not shown.)

   # Configure the 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 abc
[Device-radius-2000] key accounting abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

# Create an ISP domain and specify the RADIUS scheme 2000 as the default AAA schemes for the domain.

```
[Device] domain 2000
[Device-isp-2000] authentication default radius-scheme 2000
[Device-isp-2000] authorization default radius-scheme 2000
[Device-isp-2000] accounting default radius-scheme 2000
[Device-isp-2000] quit
```

# Configure a time range **ftp** for the weekdays from 8:00 to 18:00.

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

# Configure ACL 3000 to deny packets destined for the FTP server at 10.0.0.1 on the weekdays during business hours.

```
[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
```

# Enable 802.1X globally.

```
[Device] dot1x
```

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

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

Verifying the configuration

Use the user account to pass authentication, and then ping the FTP server on any weekday during business hours.

```
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 taken effect on the user, and the user cannot access the FTP server.

Configuring EAD fast deployment

Overview

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

EAD fast deployment enables the access device to redirect a user seeking to access the network to download and install EAD client. This function eliminates the tedious job of the administrator to deploy EAD clients.

EAD fast deployment is implemented by the following functions:

- Free IP
- URL redirection

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. An unauthenticated user can access only this segment to download EAD client, obtain a dynamic IP address from a DHCP server, or perform some other tasks to be compliant with the network security strategy.

URL redirection

If an unauthenticated 802.1X user is using a web browser to access the network, the EAD fast deployment function redirects the user to a specific URL, for example, the EAD client software download page.

The server that provides the URL must be on the free IP accessible to unauthenticated users.

Configuration prerequisites

- Enable 802.1X globally.
- Enable 802.1X on the port, and set the port authorization mode to **auto**.

Configuring a free IP

Follow these guidelines when you configure a free IP:

- When a free IP is configured, the EAD fast deployment is enabled. To allow a user to obtain a dynamic IP address before passing 802.1X authentication, make sure the DHCP server is on the free IP segment.
- When global MAC authentication, Layer-2 portal 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 that the free IP segments are in both guest VLAN and Auth-Fail VLAN. Users can access only the free IP segments.

To configure a free IP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a free IP.	**dot1x free-ip** *ip-address* { *mask-address* | *mask-length* }	By default, no free IP is configured.

Configuring the redirect URL

Follow these guidelines when you configure the redirect URL:

- The redirect URL must be on the free IP subnet.
- When Layer-2 portal is configured, the redirect URL does not take effect.

To configure a redirect URL:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the redirect URL.	**dot1x url** *url-string*	By default, no redirect URL is configured.

Setting the EAD rule timer

EAD fast deployment automatically creates an ACL rule, or an EAD rule, to open access to the redirect URL for each redirected user seeking to access the network. The EAD rule timer sets the lifetime of each ACL rule. When the 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.

To prevent ACL rule resources from being used up, you can shorten the timer when the amount of EAD users is large.

To set the EAD rule timer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the EAD rule timer.	**dot1x timer ead-timeout** *ead-timeout-value*	Optional. The default timer is 30 minutes.

Displaying and maintaining EAD fast deployment

Task	Command	Remarks
Display 802.1X session information, statistics, or configuration information.	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

EAD fast deployment configuration example

Network requirements

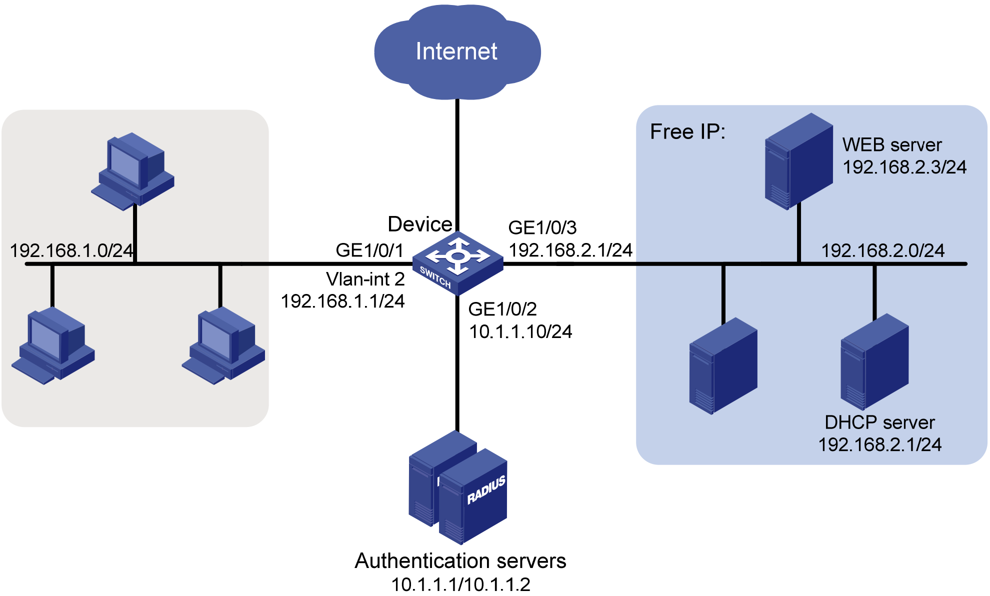
As shown in Figure 31, the hosts on the intranet 192.168.1.0/24 are attached to port GigabitEthernet 1/0/1 of the network access device, and they use DHCP to obtain IP addresses.

Deploy EAD solution for the intranet so that all hosts must pass 802.1X authentication to access the network.

To allow all intranet users to install and update 802.1X client program from a web server, configure the following:

- Allow unauthenticated users to access the segment of 192.168.2.0/24, and to obtain IP address on the segment of 192.168.1.0/24 through DHCP.
- Redirect unauthenticated users to a preconfigured web page when the users use a web browser to access any external network except 192.168.2.0/24. The web page allows users to download the 802.1X client program.
- Allow authenticated 802.1X users to access the network.

Figure 31 Network diagram



In addition to the configuration on the access device, complete the following tasks:

- Configure the DHCP server so that the host can obtain an IP address on the segment of 192.168.1.0/24.
- Configure the web server so that users can log in to the web page to download 802.1X clients.

- Configure the authentication server to provide authentication, authorization, and accounting services.

Configuration procedure

1. Configure an IP address for each interface. (Details not shown.)
2. Configure DHCP relay:

   # Enable DHCP.

   ```
   <Device> system-view
   [Device] dhcp enable
   ```

   # Configure a DHCP server for a DHCP server group.

   ```
   [Device] dhcp relay server-group 1 ip 192.168.2.2
   ```

   # Enable the relay agent on VLAN interface 2.

   ```
   [Device] interface vlan-interface 2
   [Device-Vlan-interface2] dhcp select relay
   ```

   # Correlate VLAN interface 2 to the DHCP server group.

   ```
   [Device-Vlan-interface2] dhcp relay server-select 1
   [Device-Vlan-interface2] quit
   ```
3. Configure a RADIUS scheme and an ISP domain.

   For more information about configuration procedure, see "802.1X authentication configuration example."
4. Configure 802.1X:

   # Configure the free IP.

   ```
   [Device] dot1x free-ip 192.168.2.0 24
   ```

   # Configure the redirect URL for client software download.

   ```
   [Device] dot1x url http://192.168.2.3
   ```

   # Enable 802.1X globally.

   ```
   [Device] dot1x
   ```

   # Enable 802.1X on the port.

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

Verifying the configuration

Use the **display dot1x** command to display the 802.1X configuration. After the host obtains an IP address from a DHCP server, use the **ping** command from the host to ping an IP address on the network segment specified by free IP.

```
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 that segment before passing 802.1X authentication. If you use a web browser to access any external website beyond the free IP segments, you are redirected to the web server, which provides the 802.1X client software download service. Enter the external website address in dotted decimal notation, for example, 3.3.3.3 or http://3.3.3.3, in the address bar.

Verifying the configuration

Use the **display dot1x** command to display the 802.1X configuration. After the host obtains an IP address from a DHCP server, use the **ping** command from the host to ping an IP address on the network segment specified by free IP.

```
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 that segment before passing 802.1X authentication. If you use a web browser to access any external website beyond the free IP segments, you are redirected to the web server, which provides the 802.1X client software download service. Enter the external website address in dotted decimal notation, for example, 3.3.3.3 or http://3.3.3.3, in the address bar.

Troubleshooting EAD fast deployment

Web browser users cannot be correctly redirected

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 it. If the resolution fails, the operating system sends an ARP request, but the target address is not in the dotted decimal notation. The redirection function 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

1. Enter a dotted decimal IP address that is not in any free IP segment.
2. Make sure that the network access device and the server are correctly configured.

Configuring MAC authentication

Overview

MAC authentication controls network access by authenticating source MAC addresses on a port. It does not require client software. A user does not need to input 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. This 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 approaches

You can perform MAC authentication on the access device (local authentication) or through a Remote Authentication Dial-In User Service (RADIUS) server.

Suppose a source MAC unknown packet arrives at a MAC authentication enabled port.

In the local authentication approach:

- If MAC-based accounts are used, the access device uses the source MAC address of the packet as the username and password to search its local account database for a match.
- If a shared account is used, the access device uses the shared account username and password to search its local account database for a match.

In the RADIUS authentication approach:

- If MAC-based accounts are used, the access device sends the source MAC address as the username and password to the RADIUS server for authentication.
- If a shared account is used, 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."

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 it regards the user idle. If a user connection has been idle for two consecutive intervals, the device logs the user out and stops accounting for the user.
- **Quiet timer**—Sets the interval that the device must wait before it can perform MAC authentication for a user that 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 access device waits for a response from a RADIUS server before it regards the RADIUS server unavailable. If the timer expires during MAC authentication, the user cannot access the network.

Using MAC authentication with other features

VLAN assignment

You can specify a VLAN in the user account for a MAC authentication user to control the account's access to network resources. After the user passes MAC authentication, the authentication server, either the local access device or a RADIUS server, assigns the VLAN to the port as the default VLAN. After the user logs off, the initial default VLAN, or the default VLAN configured before any VLAN is assigned by the authentication server, restores. If the authentication server assigns no VLAN, the initial default VLAN applies.

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

If MAC-based VLAN is enabled on a hybrid port, the device maps the server-assigned VLAN to the MAC address of the user. The default VLAN of the hybrid port does not change.

ACL assignment

You can specify an ACL in the user account for a MAC authentication user to control its access to network resources. After the user passes MAC authentication, the authentication server, either the local access device or a RADIUS server, assigns the ACL to the access port to filter the traffic from this user. You must configure the ACL on the access device for the ACL assignment function. You can change ACL rules while the user is online.

Guest VLAN

You can configure a guest VLAN to accommodate MAC authentication 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 anti-virus software and system patches. If no MAC authentication guest VLAN is configured, the user that fails MAC authentication cannot access any network resources.

If a user in the guest VLAN passes MAC authentication, that user is removed from the guest VLAN and can access all authorized network resources. If not, the user is still in the MAC authentication guest VLAN.

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

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 a limit set of network resources depending on your configuration.

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 RADIUS configuration, see "Configuring AAA."

Any of the following RADIUS authentication server changes in the ISP domain for MAC authentication users on a port can cause users to be removed from the critical VLAN:

- An authentication server is added to the ISP domain and the server is reachable.
- A response from a RADIUS authentication server is received.
- The RADIUS server probing function detects that a RADIUS authentication server is reachable.

Configuration task list

Task	Remarks
Basic configuration for MAC authentication: • Configuring MAC authentication globally • Configuring MAC authentication on a port	Required
Specifying a MAC authentication domain	Optional
Configuring a MAC authentication guest VLAN	Optional
Configuring a MAC authentication critical VLAN	Optional
Configuring MAC authentication delay	Optional

Basic configuration for MAC authentication

- Create and configure an authentication domain, also called "an ISP domain."
- For local authentication, create local user accounts, and specify the **lan-access** service for the accounts.
- For RADIUS authentication, check that 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 that the username and password for each account is the same as the MAC address of the MAC authentication users.

MAC authentication can take effect on a port only when it is enabled globally and on the port.

Configuring MAC authentication globally

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable MAC authentication globally.	**mac-authentication**	Disabled by default.
3.	Configure MAC authentication timers.	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }	Optional. By default, the offline detect timer is 300 seconds, the quiet timer is 60 seconds, and the server timeout timer is 100 seconds.
4.	Configure the properties of MAC authentication user accounts.	**mac-authentication user-name-format** { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*] | **mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] }	Optional. By default, the username and password for a MAC authentication user account must be a MAC address in lower case without hyphens.

NOTE:

When global MAC authentication is enabled, the EAD fast deployment function cannot take effect.

Configuring MAC authentication on a port

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable MAC authentication.	• In system view: **mac-authentication interface** *interface-list* • In interface view: a. **interface** *interface-type interface-number* b. **mac-authentication**	Disabled by default. Enable MAC authentication for ports in bulk in system view or an individual port in Ethernet interface view.
3.	Set the maximum number of concurrent MAC authentication users allowed on a port.	**mac-authentication max-user** *user-number*	Optional. By default, the maximum number of concurrent MAC authentication users is 1024.

NOTE:

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

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 specify authentication domains for MAC authentication users in the following ways:

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

MAC authentication chooses an authentication domain for users on a port in this order: the interface-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:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify an authentication domain for MAC authentication users.	• In system view: **mac-authentication domain** *domain-name* • In interface view: a. **interface** *interface-type interface-number* b. **mac-authentication domain** *domain-name*	Use either method. By default, the system default authentication domain is used for MAC authentication users.

Configuring a MAC authentication guest VLAN

Follow the guidelines in Table 10 when configuring a MAC authentication guest VLAN on a port.

Table 10 Relationships of the MAC authentication guest VLAN with other security features

Feature	Relationship description	Reference
Quiet function of MAC authentication	The MAC authentication guest VLAN function has higher priority. A user can access any resources in the guest VLAN.	See "MAC authentication timers"
Port intrusion protection	The MAC authentication guest VLAN function has higher priority than the block MAC action but lower priority than the shutdown port action of the port intrusion protection feature.	See "Configuring port security"
802.1X guest VLAN on a port that performs MAC-based access control	The MAC authentication guest VLAN has a lower priority.	See "Configuring 802.1X"

If MAC authentication clients in your network cannot trigger an immediate DHCP-assigned IP address renewal in response to a VLAN change, the MAC authentication users cannot access authorized network resources immediately after a MAC authentication is complete. As a solution, remind the MAC authentication users to release their IP addresses or repair their network connections for a DHCP reassignment after MAC authentication is complete.

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

- Enable MAC authentication.
- Enable MAC-based VLAN on the port.
- Create the VLAN to be specified as the MAC authentication guest VLAN.

To configure a MAC authentication guest VLAN:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Ethernet port view.	**interface** *interface-type interface-number*	N/A
3.	Specify a MAC authentication guest VLAN.	**mac-authentication guest-vlan** *guest-vlan-id*	By default, no MAC authentication guest VLAN is configured. You can configure only one MAC authentication guest VLAN on a port.

Configuring a MAC authentication critical VLAN

Follow the guidelines in Table 11 when you configure a MAC authentication critical VLAN on a port.

Table 11 Relationships of the MAC authentication critical VLAN with other security features

Feature	Relationship description	Reference
Quiet function of MAC authentication	The MAC authentication critical VLAN function 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, and the user's MAC address is not marked as a silent MAC address.	See "MAC authentication timers"
Port intrusion protection	The MAC authentication critical VLAN function has higher priority than the block MAC action but lower priority than the shutdown port action of the port intrusion protection feature.	See "Configuring port security"

If MAC authentication clients in your network cannot trigger an immediate DHCP-assigned IP address renewal in response to a VLAN change, the MAC authentication users cannot access authorized network resources immediately after a MAC authentication is complete. As a solution, remind the MAC authentication users to release their IP addresses or repair their network connections for a DHCP reassignment after MAC authentication is complete.

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

- Enable MAC authentication.

- Enable MAC-based VLAN on the port.
- Create the VLAN to be specified as the MAC authentication critical VLAN.

To configure a MAC authentication critical VLAN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet port view.	**interface** *interface-type interface-number*	N/A
3. Specify a MAC authentication critical VLAN.	**mac-authentication critical vlan** *critical-vlan-id*	By default, no MAC authentication critical VLAN is configured. You can configure only one MAC authentication critical VLAN on a port.

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.

To configure MAC authentication delay:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Enable MAC authentication delay and set the delay time.	**mac-authentication timer auth-delay** *time*	By default, MAC authentication is not delayed.

Displaying and maintaining MAC authentication

Task	Command	Remarks
Display MAC authentication information.	**display mac-authentication** [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear MAC authentication statistics.	**reset mac-authentication statistics** [**interface** *interface-list*]	Available in user view

MAC authentication configuration examples

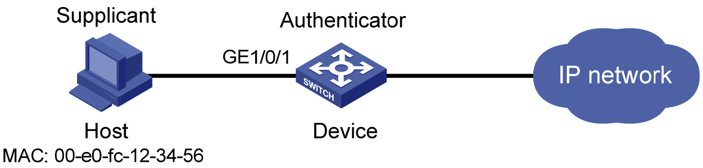
Local MAC authentication configuration example

Network requirements

In the network in Figure 32, perform local MAC authentication on port GigabitEthernet 1/0/1 to control Internet access. Make sure that:

- All users belong to domain aabbcc.net.
- Local users use their MAC address as the username and password for MAC authentication. The MAC addresses are hyphen separated and in lower case.
- The access device detects whether a user has gone offline every 180 seconds. When a user fails authentication, the device does not authenticate the user within 180 seconds.

Figure 32 Network diagram



Configuration procedure

# Add a local user account, set both the username and password to 00-e0-fc-12-34-56, the MAC address of the user host, and enable LAN access service for the account.

```
<Device> system-view
[Device] local-user 00-e0-fc-12-34-56
[Device-luser-00-e0-fc-12-34-56] password simple 00-e0-fc-12-34-56
[Device-luser-00-e0-fc-12-34-56] service-type lan-access
[Device-luser-00-e0-fc-12-34-56] quit
```

# Configure ISP domain **aabbcc.net** to perform local authentication for LAN access users.

```
[Device] domain aabbcc.net
[Device-isp-aabbcc.net] authentication lan-access local
[Device-isp-aabbcc.net] quit
```

# Enable MAC authentication globally.

```
[Device] mac-authentication
```

# Enable MAC authentication on port GigabitEthernet 1/0/1.

```
[Device] mac-authentication interface gigabitethernet 1/0/1
```

# Specify the ISP domain for MAC authentication.

```
[Device] mac-authentication domain aabbcc.net
```

# Set the MAC authentication timers.

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

# Configure MAC authentication to use MAC-based accounts. The MAC address usernames and passwords are hyphenated and in lowercase.

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

Verifying the configuration

# Display MAC authentication settings and statistics.

```
<Device> display mac-authentication
MAC address authentication is enabled.
 User name format is MAC address in lowercase, like xx-xx-xx-xx-xx-xx
 Fixed username:mac
 Fixed password:not configured
          Offline detect period is 180s
          Quiet period is 180s.
          Server response timeout value is 100s
          The max allowed user number is 1024 per slot
          Current user number amounts to 1
          Current domain is aabbcc.net
Silent Mac User info:
          MAC Addr         From Port                    Port Index
Gigabitethernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
 Max number of on-line users is 256
  Current online user number is 1
          MAC Addr         Authenticate state           Auth Index
          00e0-fc12-3456   MAC_AUTHENTICATOR_SUCCESS     29
```

# After the user passes authentication, use the **display connection** command to display the online user information.

```
<Device> display connection
Slot:  1
Index=29  ,Username=00-e0-fc-12-34-56@aabbcc.net
 IP=N/A
 IPv6=N/A
 MAC=00e0-fc12-3456
 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

RADIUS-based MAC authentication configuration example

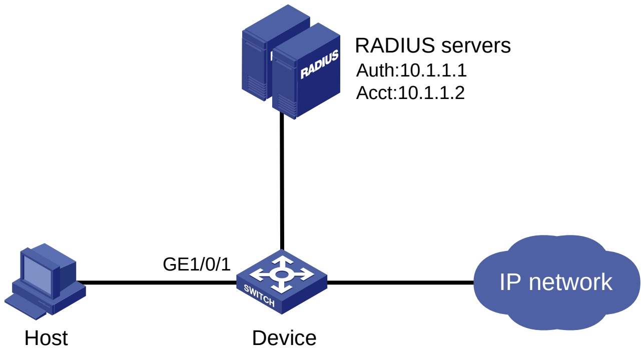
Network requirements

As shown in Figure 33, a host connects to port GigabitEthernet 1/0/1 on the access device. The device uses RADIUS servers for authentication, authorization, and accounting.

Perform MAC authentication on port GigabitEthernet 1/0/1 to control Internet access. Make sure that:

- The device detects whether a user has gone offline every 180 seconds. If a user fails authentication, the device does not authenticate the user within 180 seconds.
- All MAC authentication users belong to ISP domain 2000 and share the user account **aaa** with password **123456**.

Figure 33 Network diagram



Configuration procedure

1. Make sure the RADIUS server and the access device can reach each other.
2. Create a shared account for MAC authentication users on the RADIUS server, and set the username **aaa** and password **123456** for the account.
3. Configure 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 abc
[Device-radius-2000] key accounting abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

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

```
[Device] domain 2000
[Device-isp-2000] authentication default radius-scheme 2000
[Device-isp-2000] authorization default radius-scheme 2000
[Device-isp-2000] accounting default radius-scheme 2000
[Device-isp-2000] quit
```

   # Enable MAC authentication globally.

```
[Device] mac-authentication
```

   # Enable MAC authentication on port GigabitEthernet 1/0/1.

```
[Device] mac-authentication interface gigabitethernet 1/0/1
```

   # Specify the ISP domain for MAC authentication.

```
[Device] mac-authentication domain 2000
```

   # Set the MAC authentication timers.

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

   # Specify username **aaa** and plaintext password **123456** for the account shared by MAC authentication users.

```
[Device] mac-authentication user-name-format fixed account aaa password simple 123456
```

Verifying the configuration

# Display MAC authentication settings and statistics.

```
<Device> display mac-authentication
MAC address authentication is enabled.
User name format is fixed account
 Fixed username:aaa
 Fixed password: ******
          Offline detect period is 180s
          Quiet period is 180s.
          Server response timeout value is 100s
          The max allowed user number is 1024 per slot
          Current user number amounts to 1
          Current domain is 2000
Silent Mac User info:
         MAC ADDR               From Port           Port Index
Gigabitethernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 1, failed: 0
 Max number of on-line users is 256
  Current online user number is 1
    MAC ADDR         Authenticate state           Auth Index
    00e0-fc12-3456   MAC_AUTHENTICATOR_SUCCESS     29
```

# After a user passes MAC authentication, use the **display connection** command to display online user information.

```
<Device> display connection
Slot:  1
Index=29  ,Username=aaa@2000
 IP=N/A
 IPv6=N/A
 MAC=00e0-fc12-3456
 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

ACL assignment configuration example

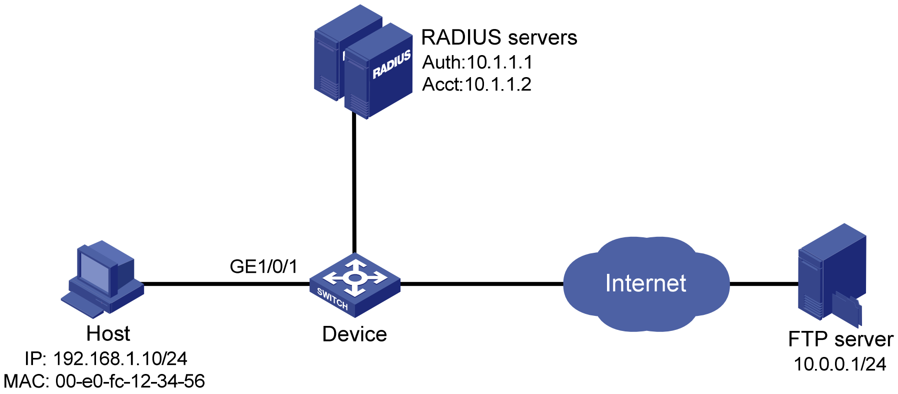
Network requirements

As shown in Figure 34, a host connects to the device's port GigabitEthernet 1/0/1, and the device uses RADIUS servers to perform authentication, authorization, and accounting.

Perform MAC authentication on port GigabitEthernet 1/0/1 to control Internet access. Make sure that an authenticated user can access the Internet but the FTP server at 10.0.0.1.

Use MAC-based user accounts for MAC authentication users. The MAC addresses are hyphen separated and in lower case.

Figure 34 Network diagram



Configuration procedure

1. Make sure the RADIUS server and the access device can reach each other.
2. Configure the ACL assignment:

   # 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
   ```
3. 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 the RADIUS scheme to an ISP domain for authentication, authorization, and accounting.

   ```
   [Sysname] domain 2000
   [Sysname-isp-2000] authentication default radius-scheme 2000
   [Sysname-isp-2000] authorization default radius-scheme 2000
   [Sysname-isp-2000] accounting default radius-scheme 2000
   [Sysname-isp-2000] quit
   ```

   # Enable MAC authentication globally.

   ```
   [Sysname] mac-authentication
   ```

   # Specify the ISP domain for MAC authentication.

   ```
   [Sysname] mac-authentication domain 2000
   ```

   # Configure the device to use MAC-based user accounts, and the MAC addresses are hyphen separated and in lowercase.

   ```
   [Sysname] mac-authentication user-name-format mac-address with-hyphen lowercase
   ```

   # Enable MAC authentication for port GigabitEthernet 1/0/1.

   ```
   [Sysname] interface gigabitethernet 1/0/1
   [Sysname-GigabitEthernet1/0/1] mac-authentication
   ```

4. Configure the RADIUS servers:

   # Add a user account with **00-e0-fc-12-34-56** as both the username and password on the RADIUS server, and specify ACL 3000 as the authorization ACL for the user account. (Details not shown.)

Verifying the configuration

After the host passes authentication, perform the **display connection** command on the device to view online user information.

```
[Sysname-GigabitEthernet1/0/1] display connection
Slot:  1
Index=9   , Username=00-e0-fc-12-34-56@2000
 IP=N/A
 IPv6=N/A
 MAC=00e0-fc12-3456

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

Ping the FTP server from the host to verify that the ACL 3000 has been assigned to port GigabitEthernet 1/0/1 to deny access to the FTP server.

```
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),
```

Configuring portal authentication

Overview

Portal authentication helps control access to the Internet. It is also called "Web authentication." A website implementing portal authentication is called a portal website.

With portal authentication, an access device redirects all users to the portal authentication page. All users can access the free services provided on the portal website; but to access the Internet, a user must pass portal authentication.

A user can access a known portal website and enter a username and password for authentication. This authentication mode is called active authentication. There is another authentication mode, forced authentication, in which the access device forces a user who is trying to access the Internet through Hypertext Transfer Protocol (HTTP) to log on to a portal website for authentication.

The portal feature provides the flexibility for Internet service providers (ISPs) to manage services. A portal website can, for example, present advertisements and deliver community and personalized services. In this way, broadband network providers, equipment vendors, and content service providers form an industrial ecological system.

Extended portal functions

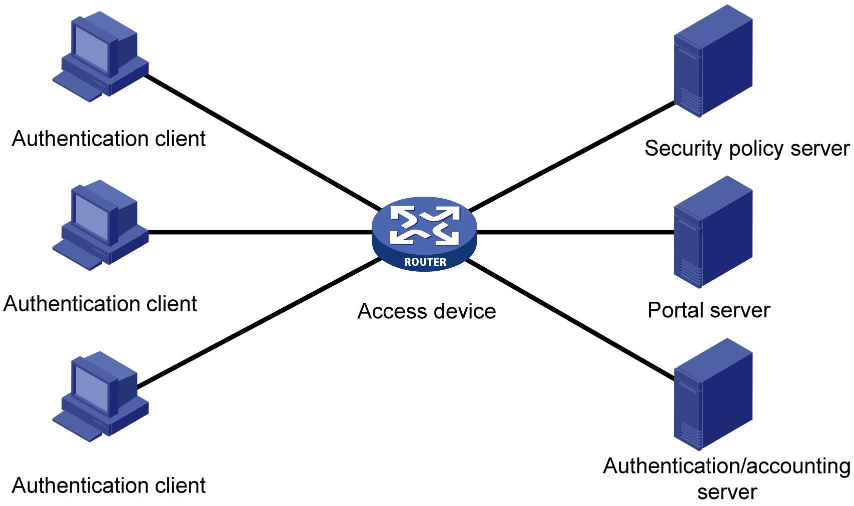
By forcing patching and anti-virus policies, extended portal functions help users to defend against viruses. Portal authentication supports the following extended functions:

- **Security check**—Works after identity authentication succeeds to check whether the required anti-virus software, virus definition file, and operating system patches are installed, and whether there is any unauthorized software installed on the user host.
- **Resource access restriction**—Allows users passing identity authentication to access only network resources in the quarantined area, such as the anti-virus server and the patch server. Only users passing both identity authentication and security check can access restricted network resources.

Portal system components

A typical portal system comprises these basic components: authentication client, access device, portal server, authentication/accounting server, and security policy server.

Figure 35 Portal system components



Authentication client

An authentication client is an entity seeking access to network resources. It is typically an end-user terminal, such as a PC. A client can use a browser or a portal client software for portal authentication. Client security check is implemented through communications between the client and the security policy server.

Access device

Access devices control user access. An access device can be a switch or router that provides the following functions:

- Redirecting all HTTP requests from unauthenticated users to the portal server.
- Interacting with the portal server, the security policy server, and the authentication/accounting server for identity authentication, security check, and accounting.
- Allowing users who have passed identity authentication and security check to access granted Internet resources.

Portal server

A portal server listens to authentication requests from authentication clients and exchanges client authentication information with the access device. It provides free portal services and pushes Web authentication pages to users.

Authentication/accounting server

An authentication/accounting server implements user authentication and accounting through interaction with the access device.

Only a RADIUS server can serve as the remote authentication/accounting server in a portal system.

Security policy server

A security policy server interacts with authentication clients and access devices for security check and resource authorization.

The components of a portal system interact in the following procedure:

1. When an unauthenticated user enters a website address in the browser's address bar to access the Internet, an HTTP request is created and sent to the access device, which redirects the HTTP request

to the portal server's Web authentication homepage. For extended portal functions, authentication clients must run the portal client software.

2. On the authentication homepage/authentication dialog box, the user enters and submits the authentication information, which the portal server then transfers to the access device.
3. Upon receipt of the authentication information, the access device communicates with the authentication/accounting server for authentication and accounting.
4. After successful authentication, the access device checks whether there is a corresponding security policy for the user. If not, it allows the user to access the Internet. Otherwise, the client communicates with the access device and the security policy server for security check. If the client passes security check, the security policy server authorizes the user to access the Internet resources.

NOTE:

To implement security check, the client must be the HP iNode client.

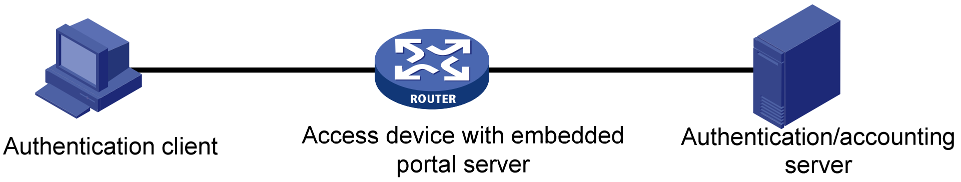
Portal authentication supports NAT traversal whether it is initiated by a Web client or an HP iNode client. When the portal authentication client is on a private network, but the portal server is on a public network and the access device is enabled with NAT, network address translations performed on the access device do not affect portal authentication. However, in such a case, HP recommends using an interface's public IP address as the source address of outgoing portal packets.

Portal system using the local portal server

System components

In addition to use a separate device as the portal server, a portal system can also use the local portal server function of the access device to authenticate Web users directly. A portal system using the local portal server does not support extended portal functions. No security policy server is needed for local portal service. In this case, the portal system consists of only three components: authentication client, access device, and authentication/accounting server, as shown in Figure 36.

Figure 36 Portal system using the local portal server


ROUTER
Authentication client
Access device with embedded portal server
Authentication/accounting server

NOTE:

The local portal server function of the access device implements only some simple portal server functions. It only allows users to log on and log off through the Web interface. It cannot take the place of an independent portal server.

Protocols used for interaction between the client and local portal server

HTTP and Hypertext Transfer Protocol Secure (HTTPS) can be used for interaction between an authentication client and an access device providing the local portal server function. 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 HTTPS packets are transferred in cipher text based on SSL.

Authentication page customization support

The local portal server function allows you to customize authentication pages. You can customize authentication pages by editing the corresponding HTML files and then compress and save the files to the storage medium of the device. A set of customized authentication pages consists of six authentication pages—the logon page, the logon success page, the online page, the logoff success page, the logon failure page, and the system busy page. A local portal server will push a corresponding authentication page at each authentication phase. If you do not customize the authentication pages, the local portal server will push the default authentication pages.

For the rules of customizing authentication pages, see "Customizing authentication pages."

Portal authentication modes

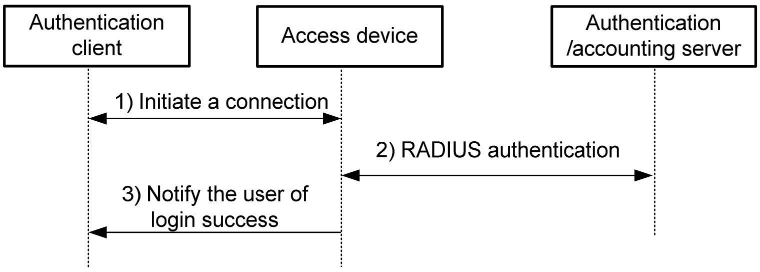
Portal authentication may work at Layer 2 or Layer 3 of the OSI model. The HP 5120 EI Switch Series supports only Layer 2 authentication mode.

You can enable Layer 2 portal authentication on an access device's Layer 2 ports that connect authentication clients, so that only clients whose MAC addresses pass authentication can access the external network. Only the local portal server provided by the access device supports Layer 2 portal authentication.

Layer 2 portal authentication allows the authentication server to assign different VLANs according to user authentication results so that access devices can thereby control user access to resources. After a client passes authentication, the authentication server can assign an authorized VLAN to allow the user to access the resources in the VLAN. If a client fails authentication, the authentication server can assign an Auth-Fail VLAN.

Layer 2 portal authentication process

Figure 37 Local Layer 2 portal authentication process



Local Layer 2 portal authentication takes the following procedure:

1. The portal authentication client sends an HTTP request. Upon receiving the HTTP request, the access device redirects it to the listening IP address of the local portal server, which supports HTTP and HTTPS requests. The local portal server pushes a Web authentication page to the authentication client. The user enters the username and password on the Web authentication page.

   The listening IP address of the local portal server is the IP address of a Layer 3 interface on the access device that can communicate with the portal client. Usually, it is a Loopback interface's IP address.

2. The access device and the RADIUS server exchange RADIUS packets to authenticate the user.

3. If the user passes RADIUS authentication, the local portal server pushes a logon success page to the authentication client.

Authorized VLAN

Layer 2 portal authentication supports VLAN assignment by the authentication server. After a user passes portal authentication, if the authentication server is configured with an authorized VLAN for the user, the authentication server assigns the authorized VLAN to the access device. Then, the access device adds the user to the authorized VLAN and generates a MAC VLAN entry. If the authorized VLAN does not exist, the access device first creates the VLAN.

By deploying the authorized VLAN assignment function, you can control which authenticated users can access which network resources.

Auth-Fail VLAN

The Auth-Fail VLAN feature allows users failing authentication to access a VLAN that accommodates network resources such as the patches server, virus definitions server, client software server, and anti-virus software server, so that the users can upgrade their client software or other programs. Such a VLAN is called an Auth-Fail VLAN.

Layer 2 portal authentication supports Auth-Fail VLAN on a port that performs MAC-based access control. With an Auth-Fail VLAN configured on a port, if a user on the port fails authentication, the access devices creates a MAC VLAN entry based on the MAC address of the user and adds the user to the Auth-Fail VLAN. Then, the user can access the non-HTTP resources in the Auth-Fail VLAN, and all HTTP requests of the user will be redirected to the authentication page. If the user passes authentication, the access device adds the user to the assigned VLAN or return the user to the initial VLAN of the port, depending on whether the authentication server assigns a VLAN. If the user fails the authentication, the access device keeps the user in the Auth-Fail VLAN. If an access port receives no traffic from a user in the Auth-Fail VLAN during a specified period of time (90 seconds by default), it removes the user from the Auth-Fail VLAN and adds the user to the initial VLAN of the port.

NOTE:

After a user is added to the authorized VLAN or Auth-Fail VLAN, the IP address of the client needs to be automatically or manually updated to make sure that the client can communicate with the hosts in the VLAN.

Assignment of authorized ACLs

The device can use ACLs to control user access to network resources and limit user access rights. With authorized ACLs specified on the authentication server, when a user passes authentication, the authentication server assigns an authorized ACL for the user, and the device filters traffic from the user on the access port according to the authorized ACL. You must configure the authorized ACLs on the access device if you specify authorized ACLs on the authentication server. To change the access right of a user, specify a different authorized ACL on the authentication server or change the rules of the corresponding authorized ACL on the device.

Portal configuration task list

Complete these tasks to configure portal authentication:

Task	Remarks
Specifying the portal server	Required

Task		Remarks
Configuring the local portal server	Customizing authentication pages	Optional
	Configuring the local portal server	Required
Enabling portal authentication		Required
Controlling access of portal users	Configuring a portal-free rule	Optional
	Setting the maximum number of online portal users	
	Specifying an authentication domain for portal users	
	Configuring portal authentication to support Web proxy	
	Enabling support for portal user moving	
Specifying an Auth-Fail VLAN for portal authentication		Optional
Specifying an auto redirection URL for authenticated portal users		Optional
Configuring portal detection functions		Optional
Logging off portal users		Optional

Configuration prerequisites

The portal feature provides a solution for user identity authentication and security check. However, the portal feature cannot implement this solution by itself. RADIUS authentication needs to be configured on the access device to cooperate with the portal feature to complete user authentication.

The prerequisites for portal authentication configuration are as follows:

- The portal server and the RADIUS server have been installed and configured properly. Local portal authentication requires no independent portal server be installed.
- The portal client, access device, and servers can reach each other.
- With RADIUS authentication, usernames and passwords of the users are configured on the RADIUS server, and the RADIUS client configurations are performed on the access device. For information about RADIUS client configuration, see "Configuring AAA."
- To implement extended portal functions, install and configure IMC EAD, and make sure that the ACLs configured on the access device correspond to those specified for the resources in the quarantined area and for the restricted resources 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 *IMC EAD Security Policy Help*.

The ACL for resources in the quarantined area and that for restricted resources correspond to isolation ACL and security ACL, respectively, on the security policy server.

You can modify the authorized ACLs on the access device. However, your changes take effect only for portal users logging on after the modification.

For portal authentication to work normally, make sure that the system name of the access device is no more than 16 characters.

Specifying the portal server

Layer 2 portal authentication uses the local portal server. Specify the IP address of a Layer 3 interface on the device that is routable to the portal client as the listening IP address of the local portal server. HP recommends using the IP address of a loopback interface, because:

- The status of a loopback interface is stable. There will be no authentication page access failures caused by interface failures.
- A loopback interface does not forward received packets to any network, avoiding impact on system performance when there are many network access requests.

To specify the local portal server for Layer 2 portal authentication:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify the listening IP address of the local portal server for Layer 2 portal authentication.	**portal local-server ip** *ip-address*	By default, no listening IP address is specified.

NOTE:

The specified listening IP address can be changed or deleted only if Layer 2 portal authentication is not enabled on any port.

Configuring the local portal server

Configuring a local portal server is required only for local portal authentication. During local portal authentication, the local portal server pushes authentication pages to users. You can define the authentication pages for users; otherwise, the default authentication pages will be used during the authentication process.

Customizing authentication pages

Customized authentication pages exist in the form of HTML files. You can compress them and then save them in the storage medium of the access device.

A set of authentication pages includes six main authentication pages and their page elements. The six main authentication pages are the logon page, the logon success page, the logon failure page, the online page, the system busy page, and the logoff success page. The page elements refer to the files that the authentication pages reference, for example, **back.jpg** for page **Logon.htm**. Each main authentication page can reference multiple page elements. If you define only some of the main authentication pages, the system will use the default authentication pages for the undefined ones.

For the local portal server to operate normally and steadily, follow the following rules when customizing authentication pages:

Rules on file names

The main authentication pages have predefined file names, which cannot be changed.

Table 12 Main authentication page file names

Main authentication page	File name
Logon page	logon.htm
Logon success page	logonSuccess.htm
Logon failure page	logonFail.htm
Online page Pushed after the user gets online for online notification	online.htm
System busy page Pushed when the system is busy or the user is in the logon process	busy.htm
Logoff success page	logoffSuccess.htm

NOTE:

You can define the names of the files other than the main authentication page files. The file names and directory names are case-insensitive.

Rules on page requests

The local portal server supports only Post and Get requests.

- Get requests are 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 are used when users submit username and password pairs, log on the system, and log off the system.

Rules on Post request attributes

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 server.
   - The username attribute is fixed as **PtUser**, and the password attribute is fixed as **PtPwd**.
   - Attribute **PtButton** is required to indicate the action that the user requests, which can be **Logon** or **Logoff**.
   - 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**.

```
<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**.

```
<form action=logon.cgi method = post >
<p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">
</form>
```

Rules on page file compression and saving

- A set of authentication page files must be compressed into a standard zip file. The name of a zip file can contain only letters, numerals, and underscores. The zip file of the default authentication pages must be saved with name **defaultfile.zip**.
- The set of authentication pages must be located in the root directory of the zip file.
- Zip files can be transferred to the device through FTP or TFTP. The default authentication pages file must be saved in the root directory of the device, and other authentication files can be saved in the root directory or the **portal** directory under the root directory of the device.

Examples of zip files on the device:

```
<Sysname> dir
Directory of flash:/portal/
   0     -rw-      1405  Feb 28 2011 15:53:31   ssid2.zip
   1     -rw-      1405  Feb 28 2011 15:53:20   ssid1.zip
   2     -rw-      1405  Feb 28 2011 15:53:39   ssid3.zip
   3     -rw-      1405  Feb 28 2011 15:53:44   ssid4.zip
2540 KB total (1319 KB free)
```

Rules on file size and contents

For the system to push customized authentication pages smoothly, you need comply with the following size and content requirements on authentication pages.

- The size of the zip file of each set of authentication pages, including the main authentication pages and the page elements, must be no more than 500 KB.
- The size of a single page, including the main authentication page and its page elements, must be no more than 50 KB before being compressed.
- Page elements can contain only static contents such as HTML, JS, CSS, and pictures.

Logging off a user who closes the logon success or online page

After a user passes authentication, the system pushes the logon success page named logonSuccess.htm. If the user initiates another authentication through the logon page, the system pushes the online page named online.htm. You can configure the device to forcibly log off the user when the user closes either of these two pages. To do so, add the following contents in logonSuccess.htm and online.htm:

1. Reference to JS file pt_private.js.
2. Function pt_unload(), which is used to trigger page unloading.
3. Function pt_submit(), the event handler function for Form.
4. Function pt_init(), which is for triggering page loading.

The following is a script example with the added contents highlighted in gray:

```
    <html>
    <head>
    <script type="text/javascript" language="javascript" src="pt_private.js"></script>
    </head>
    <body onload="pt_init();" onbeforeunload="return pt_unload();">
    ... ...
```

```
<form action=logon.cgi method = post onsubmit="pt_submit()">
    ... ...
    </body>
    </html>
```

Redirecting authenticated users to a specified Web page

To make the device automatically redirect authenticated users to a specified Web page, 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:

   ```
       <form method=post action=logon.cgi target="blank">
   ```

2. Add the function for page loading pt_init() to logonSucceess.htm.

   See the contents in gray:

   ```
       <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>
   ```

HP recommends using Microsoft IE 6.0 or above on the authentication clients. Make sure the browser of an authentication client permits pop-ups or permits pop-ups from the access device. Otherwise, the user cannot log off by closing the logon success or online page and can only click **Cancel** to return back to the logon success or online page.

If a user refreshes the logon success or online page, or jumps to another website from either of the pages, the device also logs off the user.

Only Microsoft IE, Mozilla Firefox, and Apple Safari browsers support the device to log off the user when the user closes the logon success or online page. Google Chrome, Opera, and other browsers do not support this function.

Configuring the local portal server

To make the local portal server take effect, specify the protocol to be used for communication between the portal client and local portal server.

Configuration prerequisites

To configure the local portal server to support HTTPS, complete these configurations at first:

- Configure PKI policies, obtain the CA certificate, and apply for a local certificate. For more information, see "Configuring PKI."
- Configure the SSL server policy, and specify the PKI domain to be used, which is configured in the above step. For more information, see "Configuring SSL."

When you specify the protocol for the local portal server to support, the local portal server will load the default authentication page file, which is supposed to be saved in the root directory of the device. Therefore, to make sure that the local portal server uses the user-defined default authentication pages, you must edit and save them properly. Otherwise, the system default authentication pages are used.

Configuration procedure

To configure the local portal server:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the protocol type for the local portal server to support and load the default authentication page file.	**portal local-server** { **http** | **https** **server-policy** *policy-name* }	By default, the local portal server does not support any protocol.
3.	Configure the welcome banner of the default authentication pages of the local portal server.	**portal server banner** *banner-string*	Optional. No welcome banner by default.

Enabling portal authentication

Only after you enable portal authentication on an access interface, can the access interface perform portal authentication for connected clients.

Before enabling Layer 2 portal authentication, make sure that:

- The listening IP address of the local portal server is specified.

Follow these guidelines when you enable Layer 2 portal authentication:

- To ensure normal operation of portal authentication on a Layer 2 port, do not enable port security, guest VLAN of 802.1X, or EAD fast deployment of 802.1X on the port.
- To support assignment of authorized VLANs, you must enable the MAC-based VLAN function on the port.

To enable Layer 2 portal authentication:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet port view.	**interface** *interface-type interface-number*	N/A
3.	Enable Layer 2 portal authentication on the port.	**portal local-server enable**	Not enabled by default.

Controlling access of portal users

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 and destination IP address, source MAC address, inbound interface, and VLAN. Packets matching a portal-free rule will not trigger portal authentication, so that users sending the packets can directly access the specified external websites.

For Layer 2 portal authentication, you can configure only a portal-free rule that is from any source address to any or a specified destination address. If you configure a portal-free rule that is from any source address to a specified destination address, users can access the specified address directly, without being redirected to the portal authentication page for portal authentication. Usually, you can configure the IP address of a server that provides certain services (such as software upgrading service) as the destination IP address of a portal-free rule, so that Layer 2 portal authentication users can access the services without portal authentication.

To configure a portal-free rule:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a portal-free rule.	**portal free-rule** *rule-number* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } | **any** } } | **source any** } *	N/A

NOTE:

You can only add or remove a portal-free rule. You cannot modify it.

Setting the maximum number of online portal users

You can use this feature to control the total number of online portal users in the system.

If the maximum number of online portal users to be set is less than that of the current online portal users, the limit can be set successfully and does not impact the online portal users, but the system does not allow new portal users to log on until the number drops down below the limit.

To set the maximum number of online portal users allowed in the system:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the maximum number of online portal users.	**portal max-user** *max-number*	1000 by default.

NOTE:

The maximum number of online portal users the switch actually assigns depends on the ACL resources on the switch.

Specifying an authentication domain for portal users

After you specify an authentication domain for portal users on an interface, the device uses the authentication domain for authentication, authorization, and accounting (AAA) of all portal users on the interface, ignoring the domain names carried in the usernames. This allows you to specify different authentication domains for different interfaces as needed.

To specify an authentication domain for portal users on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Specify an authentication domain for portal users on the interface.	**portal domain** *domain-name*	By default, no authentication domain is specified for portal users.

The switch selects the authentication domain for a portal user on an interface in this order: the authentication domain specified for the interface, the authentication domain carried in the username, and the system default authentication domain. For information about the default authentication domain, see "Configuring AAA."

Configuring portal authentication to support Web proxy

By default, proxied HTTP requests cannot trigger Layer 2 portal authentication but are silently dropped. To allow such HTTP requests to trigger portal authentication, configure the port numbers of the Web proxy servers on the switch.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover Web proxy servers, add the port numbers of the Web proxy servers on the switch, and configure portal-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.

You must add the port numbers of the Web proxy servers on the switch and users must make sure their browsers that use a Web proxy server do not use the proxy server for the listening IP address of the local portal server. Thus, HTTP packets that the portal user sends to the local portal server are not sent to the Web proxy server.

To configure portal authentication to support a Web proxy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Add a Web proxy server port number.	**portal web-proxy port** *port-number*	By default, no Web proxy server port number is configured and proxied HTTP requests cannot trigger portal authentication.

Enabling support for portal user moving

In scenarios where there are hubs, Layer 2 switches, or APs between users and the access devices, if an authenticated user moves from the current access port to another Layer 2-portal-authentication-enabled port of the device without logging off, the user cannot get online when the original port is still up. The reason is that the original port is still maintaining the authentication information of the user and the device does not permit such a user to get online from another port by default.

To solve the problem described above, enable support for portal user moving on the device. Then, when a user moves from a port of the device to another, the device provides services in either of the following ways:

- If the original port is still up and the two ports belong to the same VLAN, the device allows the user to continue to access the network without re-authentication, and uses the new port information for user accounting.
- If the original port is down or the two ports belong to different VLANs, the device removes the authentication information of the user from the original port and authenticates the user on the new port.

To enable support for portal user moving:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable support for portal user moving.	**portal move-mode auto**	Disabled by default

For a user with authorization information (such as authorized VLAN) configured, after the user moves from a port to another, the switch tries to assign the authorization information to the new port. If the operation fails, the switch deletes the user's information from the original port and re-authenticates the user on the new port.

Specifying an Auth-Fail VLAN for portal authentication

This task sets the Auth-Fail VLAN to be assigned to users failing portal authentication. You can specify different Auth-Fail VLANs for portal authentication on different ports. A port can be specified with only one Auth-Fail VLAN for portal authentication.

Before specifying an Auth-Fail VLAN, be sure to create the VLAN.

To specify an Auth-Fail VLAN for portal authentication:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A

Step		Command	Remarks
3.	Specify an Auth-Fail VLAN for portal authentication on the port.	**portal auth-fail vlan** *authfail-vlan-id*	Not specified by default

After you specify an Auth-Fail VLAN for portal authentication on a port, you must also enable the MAC-based VLAN function on the port to make the specified Auth-Fail VLAN take effect. For information about MAC VLAN, see *Layer 2—LAN Switching Configuration Guide*.

The MAC-VLAN entries generated in response to portal authentication failures do not overwrite the MAC-VLAN entries already generated in other authentication modes.

Specifying an auto redirection URL for authenticated portal users

After a user passes portal authentication, if the access device is configured with an auto redirection URL, it redirects the user to the URL after a specified period of time.

Follow these guidelines to specify an auto redirection URL for authenticated portal users:

- The **wait-time** *period* option is effective to only local portal authentication.
- When no auto redirection URL is specified for authenticated portal users, an authenticated user is usually redirected to the URL the user typed in the address bar before portal authentication. However, with local portal authentication, if the URL a user typed in the address bar before portal authentication is more than 255 characters, the user cannot be redirected to the page of the URL after passing portal authentication.

To specify an auto redirection URL for authenticated portal users:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Specify an auto redirection URL for authenticated portal users.	**portal redirect-url** *url-string* [**wait-time** *period*]	By default, an authenticated user is redirected to the URL the user typed in the address bar before portal authentication.

Configuring portal detection functions

After a Layer 2 portal user gets online, the device starts a detection timer for the user, and checks whether the user's MAC address entry has been aged out or the user's MAC address entry has been matched (a match means a packet has been received from the user) at the interval. If the device finds no MAC address entry for the user or receives no packets from the user during two successive detection intervals, the device considers that the user has gone offline and clears the authentication information of the user.

To set the Layer 2 portal user detection interval:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the Layer 2 portal user detection interval.	**portal offline-detect interval** *offline-detect-interval*	300 seconds by default

Logging off portal users

Logging off a user terminates the authentication process for the user or removes the user from the authenticated users list.

To log off users:

Step	Command
1. Enter system view.	**system-view**
2. Log off users.	**portal delete-user** { *ip-address* | **all** | **interface** *interface-type interface-number* }

Displaying and maintaining portal

Task	Command	Remarks
Display information about a portal-free rule or all portal-free rules.	**display portal free-rule** [*rule-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the portal configuration of an interface.	**display portal interface** *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display configuration information about the local portal server.	**display portal local-server** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display TCP spoofing statistics.	**display portal tcp-cheat statistics** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about portal users on a specific interface or all interfaces.	**display portal user** { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear TCP spoofing statistics.	**reset portal tcp-cheat statistics**	Available in user view

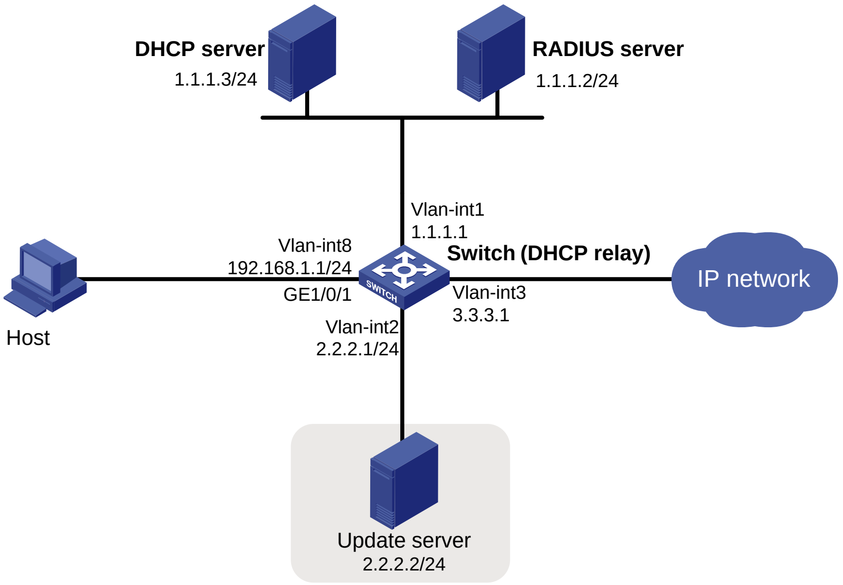
Portal configuration examples

Network requirements

As shown in Figure 38, a host is directly connected to a switch. The switch performs Layer 2 portal authentication on users connected to port GigabitEthernet 1/0/1. More specifically,

- Use the remote RADIUS server for authentication, authorization and accounting.
- Use the remote DHCP server to assign IP addresses to users.
- The listening IP address of the local portal server is 4.4.4.4. The local portal server pushes the user-defined authentication pages to users and uses HTTPS to transmit authentication data.
- Add users passing authentication to VLAN 3.
- Add users failing authentication to VLAN 2, to allow the users to access resources on the update server.
- The host obtains an IP address through DHCP. Before authentication, the DHCP server assigns an IP address in segment 192.168.1.0/24 to the host. When the host passes the authentication, the DHCP server assigns an IP address in segment 3.3.3.0/24 to the host. When the host fails authentication, the DHCP server assigns an IP address in segment 2.2.2.0/24 to the host.

Figure 38 Network diagram



Configuration procedures

Follow these guidelines to configure Layer 2 portal authentication:

- Make sure that the host, switch, and servers can reach each other before portal authentication is enabled.
- Configure the RADIUS server properly to provide normal authentication/authorization/accounting functions for users. In this example, you must create a portal user account with the account name **userpt** on the RADIUS server, and configure an authorized VLAN for the account.
- On the DHCP server, you must specify the IP address ranges (192.168.1.0/24, 3.3.3.0/24, 2.2.2.0/24), specify the default gateway addresses (192.168.1.1, 3.3.3.1, 2.2.2.1), exclude the

update server's address 2.2.2.2 from the address ranges for address allocation, specify the leases for the assigned IP addresses and make sure there is a route to the host. To shorten the IP address update time in case of an authentication state change, set a short lease for each address.

- Because the DHCP server and the DHCP client are not in the same subnet, you need to configure a DHCP relay agent on the subnet of the client. For more information about DHCP relay agent, see *Layer 3—IP Services Configuration Guide*.

Perform the following configuration on the switch to implement Layer 2 portal authentication:

1. Configure portal authentication:

   # Add Ethernet ports to related VLANs and configure IP addresses for the VLAN interfaces. (Details not shown.)

   # Configure PKI domain **pkidm**, and apply for a local certificate and CA certificate. For more configuration information, see "Configuring PKI."

   # Edit the user-defined authentication pages file, compress it into a zip file named **defaultfile**, and save the file in the root directory of the access device.

   # Configure SSL server policy **sslsvr**, and specify to use PKI domain **pkidm**.

   ```
   <Switch> system-view
   [Switch] ssl server-policy sslsvr
   [Switch-ssl-server-policy-sslsvr] pki pkidm
   [Switch-ssl-server-policy-sslsvr] quit
   ```

   # Configure the local portal server to support HTTPS and reference SSL server policy **sslsvr**.

   ```
   [Switch] portal local-server https server-policy sslsvr
   ```

   # Configure the IP address of loopback interface 12 as 4.4.4.4.

   ```
   [Switch] interface loopback 12
   [Switch-LoopBack12] ip address 4.4.4.4 32
   [Switch-LoopBack12] quit
   ```

   # Specify IP address 4.4.4.4 as the listening IP address of the local portal server for Layer 2 portal authentication.

   ```
   [Switch] portal local-server ip 4.4.4.4
   ```

   # Enable portal authentication on port GigabitEthernet 1/0/1, and specify the Auth-Fail VLAN of the port as VLAN 2.

   ```
   [Switch] interface gigabitethernet 1/0/1
   [Switch-GigabitEthernet1/0/1] port link-type hybrid
   [Switch-GigabitEthernet1/0/1] mac-vlan enable
   [Switch-GigabitEthernet1/0/1] portal local-server enable
   [Switch-GigabitEthernet1/0/1] portal auth-fail vlan 2
   [Switch-GigabitEthernet1/0/1] quit
   ```

2. Configure a RADIUS scheme:

   # Create a RADIUS scheme named **rs1** and enter its view.

   ```
   <Switch> system-view
   [Switch] radius scheme rs1
   ```

   # Set the server type for the RADIUS scheme. When using the IMC server, set the server type to **extended**.

   ```
   [Switch-radius-rs1] server-type extended
   ```

   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 1.1.1.2
[Switch-radius-rs1] primary accounting 1.1.1.2
[Switch-radius-rs1] key accounting simple radius
[Switch-radius-rs1] key authentication simple radius
[Switch-radius-rs1] quit
```

3. Configure an authentication domain:

   # Create and enter ISP domain **triple**.

   ```
   [Switch] domain triple
   ```

   # Configure AAA methods for the ISP domain.

   ```
   [Switch-isp-triple] authentication portal radius-scheme rs1
   [Switch-isp-triple] authorization portal radius-scheme rs1
   [Switch-isp-triple] accounting portal radius-scheme rs1
   [Switch-isp-triple] quit
   ```

   # Configure domain **triple** as the default ISP domain for all users. Then, if a user enters a username without any ISP domain at logon, the authentication and accounting methods of the default domain are used for the user.

   ```
   [Switch] domain default enable triple
   ```

4. Configure the DHCP relay agent:

   # Enable DHCP.

   ```
   [Switch] dhcp enable
   ```

   # Create DHCP server group 1 and add DHCP server 1.1.1.3 into the group.

   ```
   [Switch] dhcp relay server-group 1 ip 1.1.1.3
   ```

   # Enable the DHCP relay agent on VLAN-interface 8.

   ```
   [Switch] interface vlan-interface 8
   [Switch-Vlan-interface8] dhcp select relay
   ```

   # Correlate DHCP server group 1 with VLAN-interface 8.

   ```
   [Switch-Vlan-interface8] dhcp relay server-select 1
   [Switch-Vlan-interface8] quit
   ```

   # Enable the DHCP relay agent on VLAN-interface 2.

   ```
   [Switch] interface vlan-interface 2
   [Switch-Vlan-interface2] dhcp select relay
   ```

   # Correlate DHCP server group 1 with VLAN-interface 2.

   ```
   [Switch-Vlan-interface2] dhcp relay server-select 1
   [Switch-Vlan-interface2] quit
   ```

   # Enable the DHCP relay agent on VLAN-interface 3.

   ```
   [Switch] interface vlan-interface 3
   [Switch-Vlan-interface3] dhcp select relay
   ```

   # Correlate DHCP server group 1 with VLAN-interface 3.

   ```
   [Switch-Vlan-interface3] dhcp relay server-select 1
   [Switch-Vlan-interface3] quit
   ```

Verifying the configuration

Before user **userpt** accesses a Web page, the user is in VLAN 8 (the initial VLAN), and is assigned with an IP address on subnet 192.168.1.0/24. When the user accesses a Web page on the external network, the Web request will be redirected to authentication page **https://4.4.4.4/portal/logon.htm**. After entering the correct username and password, the user can pass the authentication. Then, the device will move the user from VLAN 8 to VLAN 3, the authorized VLAN. You can use the **display connection ucibindex** command to view the online user information

```
<Switch> display connection ucibindex 30
Slot:  1
Index=30  , Username=userpt@triple
MAC=0015-e9a6-7cfe
IP=192.168.1.2
IPv6=N/A
Access=PORTAL  ,AuthMethod=PAP
Port Type=Ethernet,Port Name=GigabitEthernet1/0/1
Initial VLAN=8, Authorization VLAN=3
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2009-11-26 17:40:02 ,Current=2009-11-26 17:48:21 ,Online=00h08m19s
 Total 1 connection matched.
```

Use the **display mac-vlan all** command to view the generated MAC-VLAN entries, which record the MAC addresses passing authentication and the corresponding VLANs.

```
[Switch] display mac-vlan all
  The following MAC VLAN addresses exist:
  S:Static  D:Dynamic
  MAC ADDR         MASK             VLAN ID   PRIO   STATE
  --------------------------------------------------------
  0015-e9a6-7cfe   ffff-ffff-ffff   3         0      D
  Total MAC VLAN address count:1
```

If a client fails authentication, it is added to VLAN 2. Use the previously mentioned commands to view the assigned IP address and the generated MAC-VLAN entry for the client.

Troubleshooting portal

Inconsistent keys on the access device and the portal server

Symptom

When a user is forced to access the portal server, the portal server displays a blank Web page, rather than the portal authentication page or an error message.

Analysis

The keys configured on the access device and the portal server are inconsistent, causing CHAP message exchange failure. As a result, the portal server does not display the authentication page.

Solution

- Use the **display portal server** command to display the key for the portal server on the access device and view the key for the access device on the portal server.
- Use the **portal server** command to modify the key on the access device or modify the key for the access device on the portal server to make sure that the keys are consistent.

Incorrect server port number on the access device

Symptom

After a user passes the portal authentication, you cannot force the user to log off by executing the **portal delete-user** command on the access device, but the user can log off by using the **disconnect** attribute on the authentication client.

Analysis

When you execute the **portal delete-user** command on the access device to force the user to log off, the access device actively sends a REQ_LOGOUT message to the portal server. The default listening port of the portal server is 50100. However, if the listening port configured on the access device is not 50100, the destination port of the REQ_LOGOUT message is not the actual listening port on the server, and the portal server cannot receive the REQ_LOGOUT message. As a result, you cannot force the user to log off the portal server.

When the user uses the **disconnect** attribute on the client to log off, the portal server actively sends a REQ_LOGOUT message to the access device. The source port is 50100 and the destination port of the ACK_LOGOUT message from the access device is the source port of the REQ_LOGOUT message so that the portal server can receive the ACK_LOGOUT message correctly, no matter whether the listening port is configured on the access device. The user can log off the portal server.

Solution

Use the **display portal server** command to display the listening port of the portal server configured on the access device and use the **portal server** command in the system view to modify it to make sure that it is the actual listening port of the portal server.

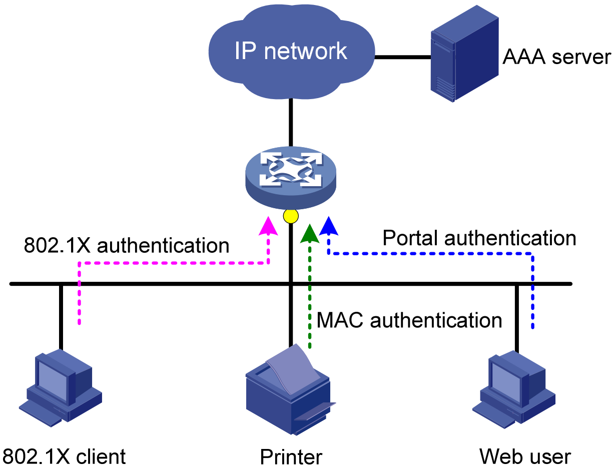
Configuring triple authentication

Overview

Triple authentication enables a Layer 2 access port to perform portal, MAC, and 802.1X authentication. A terminal can access the network if it passes one type of authentication.

Triple authentication is suitable for a LAN that comprises terminals that require different authentication services. For example, the triple authentication-enabled access port in Figure 39 can perform MAC authentication for the printer, 802.1X authentication for a PC installed with the 802.1X client, and port authentication for the other PC.

Figure 39 Triple authentication network diagram



For more information about portal authentication, MAC authentication and 802.1X authentication, see "Configuring portal authentication," "Configuring MAC authentication," and "Configuring 802.1X."

Triple authentication mechanism

The three types of authentication are triggered by different packets:

- The access port performs MAC authentication for a terminal when it receives an ARP or DHCP broadcast packet from the terminal for the first time. If the terminal passes MAC authentication, the terminal can access the network. If the MAC authentication fails, the access port performs 802.1X or portal authentication.
- The access port performs 802.1X authentication when it receives an EAP packet from an 802.1X client. If the unicast trigger function of 802.1X is enabled on the access port, any packet from an 802.1X client can trigger an 802.1X authentication.
- The access port performs portal authentication when it receives an HTTP packet from a terminal.

If a terminal triggers different types of authentication, the authentications are processed at the same time. The failure of one type of authentication does not affect the others. When a terminal passes one type of authentication, the other types of authentication being performed are terminated. Then, whether the other types of authentication can be triggered varies:

- If a terminal passes 802.1X or portal authentication, no other types of authentication will be triggered for the terminal.
- If the terminal passes MAC authentication, no portal authentication can be triggered for the terminal, but 802.1X authentication can be triggered. When the terminal passes 802.1X authentication, the 802.1X authentication information will overwrite the MAC authentication information for the terminal.

Using triple authentication with other features

A triple authentication enabled access port supports working with the following features.

VLAN assignment

After a terminal passes authentication, the authentication server assigns an authorized VLAN to the access port for the access terminal. The terminal can then access the network resources in the authorized VLAN.

Auth-Fail VLAN or MAC authentication guest VLAN

After a terminal fails authentication, the access port:

- Adds the terminal to an Auth-Fail VLAN, if it uses 802.1X or portal authentication service.
- Adds the terminal to a MAC authentication guest VLAN, if it uses MAC authentication service.

A terminal may undergo all three types of authentication. If it fails to pass all types of authentication, the access port adds the terminal to the 802.1X Auth-Fail VLAN.

ACL assignment

You can specify an authorization ACL for an authenticated user to control its access to network resources. After the user passes MAC authentication, the authentication server, either the local access device or a RADIUS server, assigns the ACL onto the access port to filter traffic for the user.

You must configure the ACLs on the access device, whether the authentication server is the access device or a remote AAA server.

Detection of online terminals

- You can enable an online detection timer, which is configurable, to detect online portal clients.
- You can enable the online handshake or periodic re-authentication function to detect online 802.1X clients at a configurable interval.
- You can enable an offline detection timer to detect online MAC authentication terminals at a configurable interval.

For more information about the extended functions, see "Configuring 802.1X," "Configuring MAC authentication," and "Configuring portal authentication."

Configuring triple authentication

Step	Command	Remarks
1. Configure 802.1X authentication.	See "Configuring 802.1X"	Configure at least one type of authentication. 802.1X authentication must use
2. Configure MAC authentication.	See "Configuring MAC authentication"	

Step	Command	Remarks
		MAC-based access control.
3. Configure Layer-2 portal authentication.	See "Configuring portal authentication"	HP does not recommend you configure 802.1X guest VLANs for triple authentication.

Triple authentication configuration examples

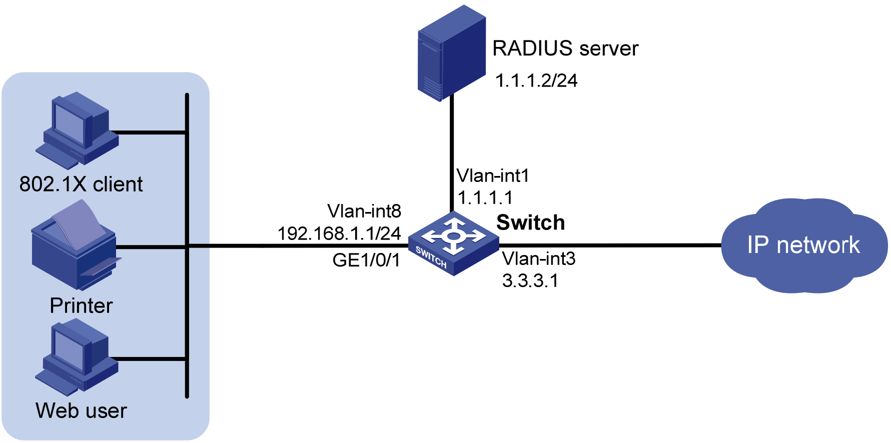
Triple authentication basic function configuration example

Network requirements

As shown in Figure 40, the terminals are connected to a switch to access the IP network. Configure triple authentication on the Layer-2 interface of the switch that connects to the terminals so that a terminal passing one of the three authentication methods, 802.1X authentication, portal authentication, and MAC authentication, can access the IP network.

- Configure static IP addresses in network 192.168.1.0/24 for the terminals.
- Use the remote RADIUS server to perform authentication, authorization, and accounting and configure the switch to send usernames carrying no ISP domain names to the RADIUS server.
- The local portal authentication server on the switch uses listening IP address 4.4.4.4. The switch sends a default authentication page to the web user and forwards authentication data using HTTP.

Figure 40 Network diagram



Configuration procedure

Make sure that the terminals, the server, and the switch can reach each other.

The host of the web user must have a route to the listening IP address of the local portal server.

1. Configure the RADIUS server, and make sure the authentication, authorization, and accounting functions work normally. In this example, configure on the RADIUS server an 802.1X user (with username **userdot**), a portal user (with username **userpt**), and a MAC authentication user (with a username and password both being the MAC address of the printer **001588f80dd7**).
2. Configure portal authentication:

   # Configure VLANs and IP addresses for the VLAN interfaces, and add ports to specific VLANs. (Details not shown.)

# Configure the local portal server to support HTTP.

```
<Switch> system-view
[Switch] portal local-server http
```

# Configure the IP address of interface loopback 0 as 4.4.4.4.

```
[Switch] interface loopback 0
[Switch-LoopBack0] ip address 4.4.4.4 32
[Switch-LoopBack0] quit
```

# Specify the listening IP address of the local portal server for Layer-2 portal authentication as 4.4.4.4.

```
[Switch] portal local-server ip 4.4.4.4
```

# Enable Layer-2 portal authentication on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] portal local-server enable
[Switch-GigabitEthernet1/0/1] quit
```

3. Configure 802.1X authentication:

# Enable 802.1X authentication globally.

```
[Switch] dot1x
```

# Enable 802.1X authentication (MAC-based access control required) on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x port-method macbased
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] quit
```

4. Configure MAC authentication:

# Enable MAC authentication globally.

```
[Switch] mac-authentication
```

# Enable MAC authentication on GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication
[Switch-GigabitEthernet1/0/1] quit
```

5. Configure a RADIUS scheme:

# Create a RADIUS scheme named **rs1**.

```
[Switch] radius scheme rs1
```

# Specify the server type for the RADIUS scheme, which must be **extended** when the IMC server is used.

```
[Switch-radius-rs1] server-type extended
```

# Specify the primary authentication and accounting servers and keys.

```
[Switch-radius-rs1] primary authentication 1.1.1.2
[Switch-radius-rs1] primary accounting 1.1.1.2
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] key accounting radius
```

# Specify usernames sent to the RADIUS server to carry no domain names.

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

6. Configure an ISP domain:

# Create an ISP domain named **triple**.

```
[Switch] domain triple
```

# Configure the default AAA methods for all types of users in the domain.

```
[Switch-isp-triple] authentication default radius-scheme rs1
[Switch-isp-triple] authorization default radius-scheme rs1
[Switch-isp-triple] accounting default radius-scheme rs1
[Switch-isp-triple] quit
```

# Configure domain **triple** as the default domain. If a username input by a user includes no ISP domain name, the authentication scheme of the default domain is used.

```
[Switch] domain default enable triple
```

Verifying the configuration

User **userdot** uses the 802.1X client to initiate authentication. After inputting the correct username and password, the user can pass 802.1X authentication. Web user **userpt** uses a web browser to access an external network. The web request is redirected to the authentication page http://4.4.4.4/portal/logon.htm. After inputting the correct username and password, the web user can pass portal authentication. The printer can pass MAC authentication after being connected to the network.

Use the **display connection** command to view online users.

```
[Switch] display connection
Slot:  1
Index=30  , Username=userpt@triple
 IP=192.168.1.2
 IPv6=N/A
 MAC=0015-e9a6-7cfe
Index=31  , Username=userdot@triple
 IP=192.168.1.3
 IPv6=N/A
 MAC=0002-0002-0001
Index=32  , Username=001588f80dd7@triple
 IP=192.168.1.4
 IPv6=N/A
 MAC=0015-88f8-0dd7

 Total 3 connection(s) matched on slot 1.
 Total 3 connection(s) matched.
```

Triple authentication supporting VLAN assignment and Auth-Fail VLAN configuration example

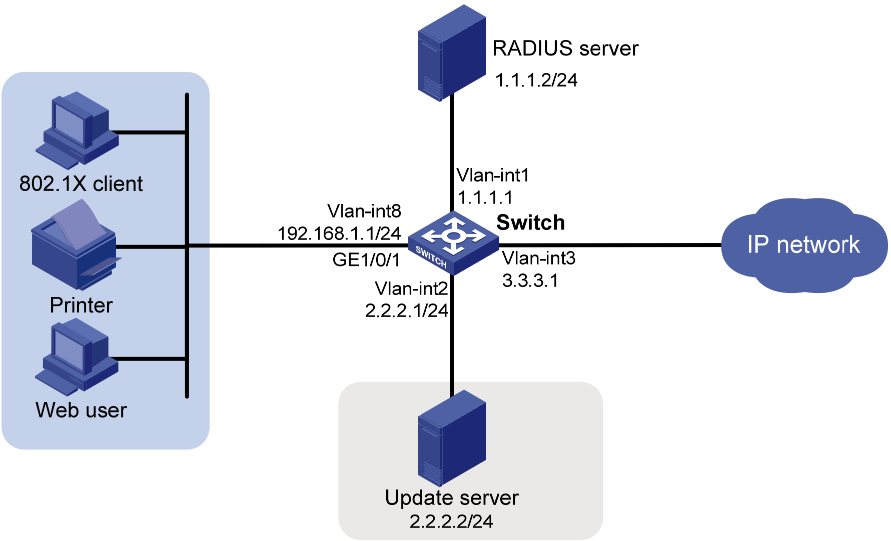
Network requirement

As shown in Figure 41, the terminals are connected to a switch to access the IP network. Configure triple authentication on the Layer-2 interface of the switch which connects to the terminals so that a terminal passing one of the three authentication methods, 802.1X authentication, portal authentication, and MAC authentication, can access the IP network.

- Portal terminals use DHCP to get IP addresses in 192.168.1.0/24 before authentication and in 3.3.3.0/24 after passing authentication.

- 802.1X terminals use IP addresses in 192.168.1.0/24 before authentication, and request IP addresses in 3.3.3.0/24 through DHCP after passing authentication. If the terminal fails authentication, it uses an IP address in 2.2.2.0/24.
- After passing authentication, the printer obtains the IP address 3.3.3.111/24 that is bound with its MAC address through DHCP.
- Use the remote RADIUS server to perform authentication, authorization, and accounting and configure the switch to remove the ISP domain names from usernames sent to the RADIUS server.
- The local portal authentication server on the switch uses listening IP address 4.4.4.4. The switch sends a default authentication page to the web user and forwards authentication data by using HTTPS.
- Configure VLAN 3 as the authorized VLAN on the RADIUS server. Users passing authentication are added to this VLAN.
- Configure VLAN 2 as the Auth-Fail VLAN on the access device. Users failing authentication are added to this VLAN, and are allowed to access only the Update server.

Figure 41 Network diagram



Configuration procedure

Make sure that the terminals, the servers, and the switch can reach each other.

When using an external DHCP server, make sure that the terminals can get IP addresses from the server before and after authentication.

1. Configure the RADIUS server, and make sure the authentication, authorization, and accounting functions work normally. In this example, configure on the RADIUS server an 802.1X user (with username **userdot**), a portal user (with username **userpt**), a MAC authentication user (with a username and password both being the MAC address of the printer **001588f80dd7**), and an authorized VLAN (VLAN 3).
2. Configure PKI domain **pkidm** and acquire the local and CA certificates. For more information, see "Configuring PKI."
3. Complete the editing of a self-defined default authentication page file, compress the file to a zip file named defaultfile and save the zip file at the root directory.
4. Configure DHCP:

# Configure VLANs and IP addresses for the VLAN interfaces, and add ports to specific VLANs. (Details not shown.)

# Enable DHCP.

```
<Switch> system-view
[Switch] dhcp enable
```

# Exclude the IP address of the update server from assignment.

```
[Switch] dhcp server forbidden-ip 2.2.2.2
```

# Configure IP address pool 1, including the address range, lease and gateway address. A short lease is recommended to shorten the time terminals use to re-acquire IP addresses after the terminals passing or failing authentication.

```
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] network 192.168.1.0 mask 255.255.255.0
[Switch-dhcp-pool-1] expired day 0 hour 0 minute 1
[Switch-dhcp-pool-1] gateway-list 192.168.1.1
[Switch-dhcp-pool-1] quit
```

A short lease is recommended to shorten the time that terminals use to re-acquire IP addresses after passing or failing authentication. However, in some applications, a terminal can require a new IP address before the lease duration expires. For example, the iNode 802.1X client automatically renews its IP address after disconnecting from the server.

# Configure IP address pool 2, including the address range, lease and gateway address. A short lease is recommended to shorten the time terminals use to re-acquire IP addresses after the terminals pass authentication.

```
[Switch] dhcp server ip-pool 2
[Switch-dhcp-pool-2] network 2.2.2.0 mask 255.255.255.0
[Switch-dhcp-pool-2] expired day 0 hour 0 minute 1
[Switch-dhcp-pool-2] gateway-list 2.2.2.1
[Switch-dhcp-pool-2] quit
```

# Configure IP address pool 3, including the address range, lease and gateway address. A short lease is recommended to shorten the time terminals use to re-acquire IP addresses after the terminals are offline.

```
[Switch] dhcp server ip-pool 3
[Switch-dhcp-pool-3] network 3.3.3.0 mask 255.255.255.0
[Switch-dhcp-pool-3] expired day 0 hour 0 minute 1
[Switch-dhcp-pool-3] gateway-list 3.3.3.1
[Switch-dhcp-pool-3] quit
```

# Configure IP address pool 4, and bind the printer MAC address 0015-e9a6-7cfe to the IP address 3.3.3.111/24 in this address pool.

```
[Switch] dhcp server ip-pool 4
[Switch-dhcp-pool-4] static-bind ip-address 3.3.3.111 mask 255.255.255.0
[Switch-dhcp-pool-4] static-bind mac-address 0015-e9a6-7cfe
[Switch-dhcp-pool-4] quit
```

5. Configure portal authentication:

# Create SSL server policy **sslsvr** and specify it to use PKI domain **pkidm**.

```
[Switch] ssl server-policy sslsvr
[Switch-ssl-server-policy-sslsvr] pki pkidm
[Switch-ssl-server-policy-sslsvr] quit
```

# Configure the local portal server to support HTTPS and use SSL server policy **sslsvr**.

```
[Switch] portal local-server https server-policy sslsvr
```

# Configure IP address 4.4.4.4 for interface loopback 12.

```
[Switch] interface loopback 12
[Switch-LoopBack12] ip address 4.4.4.4 32
[Switch-LoopBack12] quit
```

# Specify the listening IP address of the local portal server as 4.4.4.4.

```
[Switch] portal local-server ip 4.4.4.4
```

# Enable Layer-2 portal authentication on GigabitEthernet 1/0/1 and specify VLAN 2 as the Auth-Fail VLAN, to which terminals failing authentication are added.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] mac-vlan enable
[Switch-GigabitEthernet1/0/1] portal local-server enable
[Switch-GigabitEthernet1/0/1] portal auth-fail vlan 2
[Switch-GigabitEthernet1/0/1] quit
```

6. Configure 802.1X authentication:

# Enable 802.1X authentication globally.

```
[Switch] dot1x
```

# Enable 802.1X authentication (MAC-based access control required) on GigabitEthernet 1/0/1, and specify VLAN 2 as the Auth-Fail VLAN.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dot1x port-method macbased
[Switch-GigabitEthernet1/0/1] dot1x
[Switch-GigabitEthernet1/0/1] dot1x auth-fail vlan 2
[Switch-GigabitEthernet1/0/1] quit
```

7. Configure MAC authentication:

# Enable MAC authentication globally.

```
[Switch] mac-authentication
```

# Enable MAC authentication on GigabitEthernet 1/0/1, and specify VLAN 2 as the Auth-Fail VLAN

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] mac-authentication
[Switch-GigabitEthernet1/0/1] mac-authentication guest-vlan 2
[Switch-GigabitEthernet1/0/1] quit
```

8. Configure a RADIUS scheme:

# Create a RADIUS scheme named **rs1**.

```
[Switch] radius scheme rs1
```

# Specify the server type for the RADIUS scheme, which must be **extended** when the IMC server is used.

```
[Switch-radius-rs1] server-type extended
```

# Specify the primary authentication and accounting servers and keys.

```
[Switch-radius-rs1] primary authentication 1.1.1.2
[Switch-radius-rs1] primary accounting 1.1.1.2
[Switch-radius-rs1] key authentication radius
[Switch-radius-rs1] key accounting radius
```

# Specify usernames sent to the RADIUS server to carry no domain names.

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

9. Configure an ISP domain:

   # Create an ISP domain named triple.

   ```
   [Switch] domain triple
   ```

   # Configure the default AAA methods for all types of users in the domain.

   ```
   [Switch-isp-triple] authentication default radius-scheme rs1
   [Switch-isp-triple] authorization default radius-scheme rs1
   [Switch-isp-triple] accounting default radius-scheme rs1
   [Switch-isp-triple] quit
   ```

   # Configure domain **triple** as the default domain. If a username input by a user includes no ISP domain name, the authentication scheme of the default domain is used.

   ```
   [Switch] domain default enable triple
   ```

Verifying the configuration

User **userdot** uses the 802.1X client to initiate authentication. After inputting the correct username and password, the user can pass 802.1X authentication. Web user **userpt** uses a web browser to access an external network. The web request is redirected to the authentication page http://4.4.4.4/portal/logon.htm. After inputting the correct username and password, the web user can pass portal authentication. The printer can pass MAC authentication after being connected to the network.

Use the **display connection** command to view connection information about online users.

```
[Switch] display connection
Slot:  1
Index=30  , Username=userpt@triple
 IP=192.168.1.2
 IPv6=N/A
 MAC=0015-e9a6-7cfe
Index=31  , Username=userdot@triple
 IP=3.3.3.2
 IPv6=N/A
 MAC=0002-0002-0001
Index=32  , Username=001588f80dd7@triple
 IP=N/A
 IPv6=N/A
 MAC=0015-88f8-0dd7

 Total 3 connection(s) matched on slot 1.
 Total 3 connection(s) matched.
```

Use the **display mac-vlan all** command to view the MAC-VLAN entries of online users. VLAN 3 is the authorized VLAN.

```
[Switch] display mac-vlan all
  The following MAC VLAN addresses exist:
  S:Static  D:Dynamic
  MAC ADDR         MASK             VLAN ID   PRIO   STATE
  --------------------------------------------------------
  0015-e9a6-7cfe   ffff-ffff-ffff   3         0      D
```

```
  0002-0002-0001   ffff-ffff-ffff   3         0      D
  0015-88f8-0dd7   ffff-ffff-ffff   3         0      D
  Total MAC VLAN address count:3
```

Use the **display dhcp server ip-in-use** command to view the IP addresses assigned to online users.

```
[Switch] display dhcp server ip-in-use all
Pool utilization: 0.59%
 IP address       Client-identifier/    Lease expiration          Type
                  Hardware address
 3.3.3.111        0015-88f8-0dd7        Dec 15 2009 17:40:52      Auto:COMMITTED
 3.3.3.2          0002-0002-0001        Dec 15 2009 17:41:02      Auto:COMMITTED
 3.3.3.3          0015-e9a6-7cfe        Unlimited                 Manual

 --- total 3 entry ---
```

When a terminal fails authentication, it is added to VLAN 2. You can also use the display commands to view the MAC-VLAN entry and IP address of the terminal.

Configuring port security

Overview

Port security combines and extends 802.1X and MAC authentication to provide MAC-based network access control. It applies to a network that requires different authentication methods for different users on a port.

Port security prevents unauthorized access to the network by checking the source MAC address of inbound traffic and prevents access to unauthorized devices by checking the destination MAC address of outbound traffic.

Port security can control MAC address learning and authentication on a port to make sure that the port learns only 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 can automatically take a pre-defined action on illegal frames. This automatic mechanism enhances network security and reduces human intervention.

NOTE:

For scenarios that require only 802.1X authentication or MAC authentication, HP recommends you configure 802.1X authentication or MAC authentication rather than port security. 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 guarantees that frames are sent only to hosts that have passed authentication or 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 pre-defined 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 three minutes (not user configurable).

Port security traps

You can configure the port security module to send traps for port security events such as login, logoff, and MAC authentication. These traps help you monitor user behaviors.

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 pre-defined NTK, intrusion protection, or trapping action.

The maximum number of users a port supports equals the maximum number of MAC addresses that port security allows or the maximum number of concurrent users the authentication mode in use allows, whichever is smaller. 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 13 describes the port security modes and the security features.

Table 13 Port security modes

Purpose	Security mode		Features that can be triggered
Turning off the port security feature	noRestrictions (the default mode) In this mode, port security is disabled on the port and access to the port is not restricted.		N/A
Controlling MAC address learning	autoLearn		NTK/intrusion protection
	secure		
Performing 802.1X authentication	userLogin		N/A
	userLoginSecure		NTK/intrusion protection
	userLoginSecureExt		
	userLoginWithOUI		
Performing MAC authentication	macAddressWithRadius		NTK/intrusion protection
Performing a combination of MAC authentication and 802.1X authentication	Or	macAddressOrUserLoginSecure	NTK/intrusion protection
		macAddressOrUserLoginSecureExt	
	Else	macAddressElseUserLoginSecure	
		macAddressElseUserLoginSecureExt	

TIP:

- **userLogin** specifies 802.1X authentication and port-based access control.
- **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.
- Typically, in a security mode with **Or**, the authentication method to be used depends on the protocol type of the authentication request.
- **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.

Controlling MAC address learning

- autoLearn

  A port in this mode can learn MAC addresses, and allows frames from learned or configured MAC addresses to pass. The automatically learned MAC addresses are secure MAC addresses. You can also configure secure MAC addresses by using the **port-security mac-address security** command. A secure MAC address never ages out by default.

  When the number of secure MAC addresses reaches the upper limit, the port transitions to secure mode.

  The dynamic MAC address learning function in MAC address management is disabled on ports operating in autoLearn mode, but you can configure MAC addresses by using the **mac-address dynamic** and **mac-address static** commands.

- 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 secure MAC addresses and manually configured MAC addresses to pass.

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. If one 802.1X user passes authentication, all the other 802.1X users of the port can access the network 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 organizationally unique identifier (OUI).

  For wired users, the port performs 802.1X authentication upon receiving 802.1X frames, and performs OUI check upon receiving non-802.1X frames.

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.

  For wired users, the port performs MAC authentication upon receiving non-802.1X frames and performs 802.1X authentication upon receiving 802.1X frames.

- macAddressOrUserLoginSecureExt

This mode is similar to the macAddressOrUserLoginSecure mode except that a port in 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.

  For wired users, the port performs MAC authentication upon receiving non-802.1X frames and performs MAC authentication and then, if the authentication fails, 802.1X authentication upon receiving 802.1X frames.

- macAddressElseUserLoginSecureExt

  This mode is similar to the macAddressElseUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users as the keyword **Ext** implies.

NOTE:

An OUI, as defined by the IEEE, is the first 24 bits of the MAC address, which uniquely identifies a device vendor.

Working with guest VLAN and Auth-Fail VLAN

An 802.1X guest VLAN is the VLAN that a user is in before initiating authentication. An 802.1X Auth-Fail VLAN or a MAC authentication guest VLAN is the VLAN that a user is in after failing authentication. Support for the guest VLAN and Auth-Fail VLAN features varies with security modes.

- You can use the 802.1X guest VLAN and 802.1X Auth-Fail VLAN features together with port security modes that support 802.1X authentication. For more information about the 802.1X guest VLAN and Auth-Fail VLAN on a port that performs MAC-based access control, see "Configuring 802.1X."
- You can use the MAC authentication VLAN feature together with security modes that support MAC authentication. For more information about the MAC authentication guest VLAN, see "Configuring MAC authentication."
- If you configure both an 802.1X Auth-Fail VLAN and a MAC authentication guest VLAN on a port that performs MAC-based access control, the 802.1X Auth-Fail VLAN has a higher priority.

Configuration task list

Task	Remarks
Enabling port security	Required.
Setting port security's limit on the number of MAC addresses on a port	Optional.
Setting the port security mode	Required.
Configuring port security features: • Configuring NTK • Configuring intrusion protection • Enabling port security traps	Optional. Configure one or more features as required.
Configuring secure MAC addresses	Optional.
Ignoring authorization information	Optional.

Enabling port security

Enabling or disabling port security resets the following security settings to the default:

- 802.1X access control mode is MAC-based, and the port authorization state is auto.
- Port security mode is noRestrictions.

When port security is enabled, you cannot manually enable 802.1X or MAC authentication, or change the access control mode or port authorization state. The port security automatically modifies these settings in different security modes.

You cannot disable port security when online users are present.

Before enabling port security, disable 802.1X and MAC authentication globally.

To enable port security:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable port security.	**port-security enable**	By default, the port security is disabled.

For more information about 802.1X configuration, see "Configuring 802.1X." For more information about MAC authentication configuration, see "Configuring MAC authentication."

Setting port security's limit on the number of MAC addresses on a port

You can set the maximum number of MAC addresses that port security allows on a port for the following purposes:

- Controlling the number of concurrent users on the port. The maximum number of concurrent users on the port equals this limit or the limit of the authentication mode (802.1X for example) in use, whichever is smaller.
- Controlling the number of secure MAC addresses on the port in autoLearn mode.

The port security's limit on the number of MAC addresses on a port is independent of the MAC learning limit described in MAC address table configuration in the *Layer 2—LAN Switching Configuration Guide*.

To set the maximum number of secure MAC addresses allowed on a port:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3.	Set the limit of port security on the number of MAC addresses.	**port-security max-mac-count** *count-value*	Not limited by default.

Setting the port security mode

After enabling port security, you can change the port security mode of a port only when the port is operating in noRestrictions (the default) mode. To change the port security mode for a port in any other mode, first use the **undo port-security port-mode** command to restore the default port security mode.

You can specify a port security mode when port security is disabled, but your configuration cannot take effect.

You cannot change the port security mode of a port when online users are present.

Configuration prerequisites

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.
- If you are configuring the autoLearn mode, set port security's limit on the number of MAC addresses. You cannot change the setting when the port is operating in autoLearn mode.

Configuration procedure

To enable a port security mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set an OUI value for user authentication.	**port-security oui** *oui-value* **index** *index-value*	Required for the **userlogin-withoui** mode. Not configured by default. To set multiple OUI values, repeat this step.
3. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
4. Set the port security mode.	**port-security port-mode** { **autolearn** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }	By default, a port operates in noRestrictions mode.

Configuring port security features

Configuring NTK

The NTK feature checks the destination MAC addresses in outbound frames to make sure that frames are forwarded only to authenticated devices. Any unicast frame with an unknown destination MAC address is discarded. Not all port security modes support triggering the NTK feature. For more information, see Table 13.

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.

To configure the NTK feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the NTK feature.	**port-security ntk-mode** { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }	By default, NTK is disabled on a port and all frames are allowed to be sent.

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 addresses list and discards the frames. All subsequent frames sourced from a blocked MAC address will be dropped. A blocked MAC address is restored to normal state after being blocked for three 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 specific period of time. The period can be configured with the **port-security timer disableport** command.

On a port operating in either the macAddressElseUserLoginSecure mode or the macAddressElseUserLoginSecureExt mode, intrusion protection is triggered only after both MAC authentication and 802.1X authentication for the same frame fail.

To configure the intrusion protection feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the intrusion protection feature.	**port-security intrusion-mode** { **blockmac** | **disableport** | **disableport-temporarily** }	By default, intrusion protection is disabled.
4. Return to system view.	**quit**	N/A
5. Set the silence timeout period during which a port remains disabled.	**port-security timer disableport** *time-value*	Optional. 20 seconds by default.

Enabling port security traps

You can configure the port security module to send traps for the following categories of events:

- **addresslearned**—Learning of new MAC addresses.
- **dot1xlogfailure/dot1xlogon/dot1xlogoff**—802.1X authentication failure, success, and 802.1X user logoff.
- **ralmlogfailure**/**ralmlogon/ralmlogoff**—MAC authentication failure, MAC authentication user logon, and MAC authentication user logoff.
- **intrusion**—Detection of illegal frames.

To enable port security traps:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable port security traps.	**port-security trap** { **addresslearned** | **dot1xlogfailure** | **dot1xlogoff** | **dot1xlogon** | **intrusion** | **ralmlogfailure** | **ralmlogoff** | **ralmlogon** }	By default, port security traps are disabled.

Configuring secure MAC addresses

Secure MAC addresses are configured or learned in autoLearn mode and can survive link down/up events. You can bind a secure MAC address to only one port in a VLAN.

IMPORTANT:

When the maximum number of secure MAC address entries is reached, the port changes to secure mode, and no more secure MAC addresses can be added or learned. The port allows only frames sourced from a secure MAC address or a MAC address configured by using the **mac-address dynamic** or **mac-address static** command to pass through.

Secure MAC addresses fall into static, sticky and dynamic secure MAC addresses.

Table 14 A comparison of static, sticky, and dynamic secure MAC addresses

Type	Address sources	Aging mechanism	Can be saved and survive a device reboot?
Static	Manually added	Not available. They never age out unless you manually remove them, change the port security mode, or disable the port security feature.	Yes.
Sticky	Manually added or automatically learned when the dynamic secure MAC function (**port-security mac-address dynamic**) is disabled.	Sticky MAC addresses by default do not age out, but you can configure an aging timer or use the aging timer together with the inactivity aging function to delete old sticky MAC addresses: • If only an aging timer is configured, the aging timer counts up regardless of whether traffic data has been sent from the sticky MAC address. • If both an aging timer and the inactivity aging function are configured, the aging timer restarts once traffic data is detected from the sticky MAC address.	Yes. The secure MAC aging timer restarts at a reboot.
Dynamic	Converted from sticky MAC addresses or automatically learned after the dynamic secure MAC function is enabled.	Same as sticky MAC addresses.	No. All dynamic secure MAC addresses are lost at reboot.

Configuration prerequisites

- 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.

Configuration procedure

To configure a secure MAC address:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the secure MAC aging timer.	**port-security timer autolearn aging** *time-value*	Optional. By default, secure MAC addresses do note age out, and you can remove them only by performing the **undo port-security mac-address security** command, changing the port security mode, or disabling the port security feature.

Step	Command	Remarks
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 interface view:** a. **interface** *interface-type interface-number* b. **port-security mac-address security** [**sticky**] *mac-address* **vlan** *vlan-id* c. **quit**	Use either method. No secure MAC address exists by default.
4. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
5. Enable inactivity aging.	**port-security mac-address aging-type inactivity**	Optional. By default, the inactivity aging function is disabled.
6. Enable the dynamic secure MAC function.	**port-security mac-address dynamic**	Optional. By default, sticky MAC addresses can be saved to the configuration file, and once saved, can survive a device reboot.

NOTE:

You can display dynamic secure MAC addresses only by using the **display port-security mac-address security** command.

Ignoring authorization information

The authorization information is delivered by the RADIUS server or the local device to an 802.1X user or MAC authenticated user who passes RADIUS or local authentication. You can configure a port to ignore the authorization information.

To configure a port to ignore the authorization information:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Ignore the authorization information from the RADIUS server or the local device.	**port-security authorization ignore**	By default, a port uses the authorization information from the RADIUS server or the local device.

Displaying and maintaining port security

Task	Command	Remarks
Display port security configuration information, operation information, and statistics about one or more ports or all ports.	**display port-security** [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about secure MAC addresses.	**display port-security mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about blocked MAC addresses.	**display port-security mac-address block** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Port security configuration examples

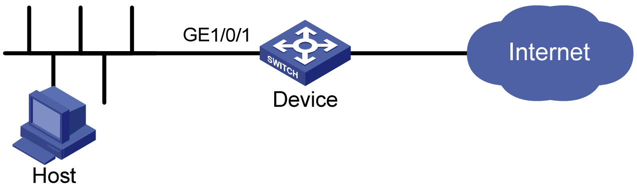
Configuring the autoLearn mode

Network requirements

See Figure 42. Configure port GigabitEthernet 1/0/1 on the Device, as follows:

- Accept up to 64 users on the port without authentication.
- Permit the port to learn and add MAC addresses as sticky MAC addresses, and set the sticky MAC aging timer to 30 minutes.
- After the number of secure MAC addresses reaches 64, the port stops learning MAC addresses. If any frame with an unknown MAC address arrives, intrusion protection starts, and the port shuts down and stays silent for 30 seconds.

Figure 42 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
```

# Enable intrusion protection traps on port GigabitEthernet 1/0/1.

```
[Device] port-security trap intrusion
[Device] interface gigabitethernet 1/0/1
```

# Set port security's limit on the number of MAC addresses to 64 on the port.

```
[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

# Display the port security configuration.

```
<Device> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Intrusion trap is enabled
AutoLearn aging time is 30 minutes
 Disableport Timeout: 30s
 OUI value:

GigabitEthernet1/0/1 is link-up
   Port mode is autoLearn
   NeedToKnow mode is disabled
   Intrusion Protection mode is DisablePortTemporarily
   Max MAC address number is 64
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

The output shows that the port security's limit on the number of secure MAC addresses on the port is 64, the port security mode is autoLearn, intrusion protection traps are enabled, and the intrusion protection action is disabling the port (DisablePortTemporarily) for 30 seconds.

# Repeatedly perform the **display port-security** command to track the number of MAC addresses learned by the port, or use the **display this** command in Layer 2 Ethernet interface view to display the secure MAC addresses.

```
<Device> system-view
[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
#
```

Execute the **display port-security interface** command after the number of MAC addresses learned by the port reaches 64, and you can see that the port security mode has changed to secure. When any frame with a new MAC address arrives, intrusion protection is triggered and you can see the following trap message.

```
#Jan 14 10:39:47:135 2011 Device PORTSEC/4/VIOLATION: Trap1.3.6.1.4.1.25506.2.26.1.
3.2:
 An intrusion occurs!
 IfIndex: 9437185
 Port: 9437185
 MAC Addr: 00:02:00:00:00:32
 VLAN ID: 1
 IfAdminStatus: 1
```

# Execute the **display interface** command, and can see that the port security feature has disabled the port.

```
[Device-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
 GigabitEthernet1/0/1 current state: DOWN (  Port Security Disabled  )
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: GigabitEthernet1/0/1 Interface
 ......
```

The port should be re-enabled 30 seconds later.

```
[Device-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
 GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: GigabitEthernet1/0/1 Interface
 ......
```

Delete several secure MAC addresses, and you can see that the port security mode of the port changes to autoLearn, and the port can learn MAC addresses again.

Configuring the userLoginWithOUI mode

Network requirements

As shown in Figure 43, 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.

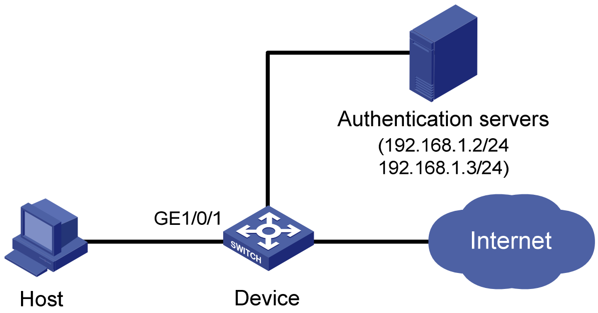
- The RADIUS server at 192.168.1.2 functions as the primary authentication server and the secondary accounting server, and the RADIUS server at 192.168.1.3 functions as the secondary authentication server and the primary accounting server. The shared key for authentication is name, and that for accounting is money.
- All users use the default authentication, authorization, and accounting methods of ISP domain **sun**, which can accommodate up to 30 users.
- The RADIUS server response timeout time is five seconds and the maximum number of RADIUS packet retransmission attempts is five. The Device sends real-time accounting packets to the RADIUS server at an interval of 15 minutes, 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 to be authenticated.

- Allow up to 16 OUI values to be configured and allow one terminal that uses any of the OUI values to access the port in addition to an 802.1X user.

Figure 43 Network diagram



Configuration procedure

Configurations on the host and RADIUS servers are not shown. The following configuration steps cover some AAA/RADIUS configuration commands. For more information about the commands, see *Security Command Referenced*.

1. Configure the RADIUS protocol:

   # 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 name
   [Device-radius-radsun] key accounting 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** to use RADIUS scheme **radsun** for authentication, authorization, and accounting of all types of users. Specify that the ISP domain can contain up to 30 users.

   ```
   [Device] domain sun
   [Device-isp-sun] authentication default radius-scheme radsun
   [Device-isp-sun] authorization default radius-scheme radsun
   [Device-isp-sun] accounting default radius-scheme radsun
   [Device-isp-sun] access-limit enable 30
   [Device-isp-sun] quit
   ```

2. Configure 802.1X:

   # Set the 802.1X authentication method to CHAP. (This configuration is optional. By default, the authentication method is CHAP for 802.1X.)

   ```
   [Device] dot1x authentication-method chap
   ```

3. Configure port security:

   # Enable port security.

```
[Device] port-security enable
```

# Add five OUI values.

```
[Device] port-security oui 1234-0100-1111 index 1
[Device] port-security oui 1234-0200-1111 index 2
[Device] port-security oui 1234-0300-1111 index 3
[Device] port-security oui 1234-0400-1111 index 4
[Device] port-security oui 1234-0500-1111 index 5
[Device] interface gigabitethernet 1/0/1
```

# Set the port security mode to userLoginWithOUI.

```
[Device-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
```

Verifying the configuration

# Display the RADIUS scheme **radsun**.

```
<Device> display radius scheme radsun
SchemeName  : radsun
  Index : 1                            Type : standard
  Primary Auth Server:
    IP: 192.168.1.2                             Port: 1812   State: active
    Encryption Key : N/A
    Probe username : N/A
    Probe interval : N/A
  Primary Acct Server:
    IP: 192.168.1.3                             Port: 1813   State: active
    Encryption Key : N/A
  Second Auth Server:
    IP: 192.168.1.3                             Port: 1812   State: active
    Encryption Key : N/A
    Probe username : N/A
    Probe interval : N/A
  Second Acct Server:
    IP: 192.168.1.2                             Port: 1813   State: active
    Encryption Key : N/A
  Auth Server Encryption Key : ******
  Acct Server Encryption Key : ******
  Accounting-On packet disable, send times : 5 , interval : 3s
  Interval for timeout(second)                           : 5
  Retransmission times for timeout                       : 5
  Interval for realtime accounting(minute)               : 15
  Retransmission times of realtime-accounting packet     : 5
  Retransmission times of stop-accounting packet         : 500
  Quiet-interval(min)                                    : 5
  Username format                                        : without-domain
  Data flow unit                                         : Byte
  Packet unit                                            : one
```

# Display the configuration of the ISP domain **sun**.

```
<Device> display domain sun
   Domain : sun
   State : Active
   Access-limit : 30
   Accounting method : Required
   Default authentication scheme      : radius:radsun
   Default authorization scheme       : radius:radsun
   Default accounting scheme          : radius:radsun
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes:
```

# Display the port security configuration.

```
<Device> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 Disableport Timeout: 20s
 OUI value:
   Index is 1,  OUI value is 123401
   Index is 2,  OUI value is 123402
   Index is 3,  OUI value is 123403
   Index is 4,  OUI value is 123404
   Index is 5,  OUI value is 123405

 GigabitEthernet1/0/1 is link-up
   Port mode is userLoginWithOUI
   NeedToKnow mode is disabled
   Intrusion Protection mode is NoAction
   Max MAC address number is not configured
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

After an 802.1X user gets online, you can see that the number of secure MAC addresses stored is 1.

# Display 802.1X information.

```
<Device> display dot1x interface gigabitethernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 EAD quick deploy is disabled

  Configuration: Transmit Period   30 s,  Handshake Period       15 s
                  Quiet Period      60 s,  Quiet Period Timer is disabled
                  Supp Timeout      30 s,  Server Timeout        100 s
                  Reauth Period   3600 s
                  The maximal retransmitting times    2
  EAD quick deploy configuration:
                EAD timeout:    30m

 The maximum 802.1X user resource number is 1024 per slot
 Total current used 802.1X resource number is 1
 GigabitEthernet1/0/1  is link-up
   802.1X protocol is enabled
   Handshake is enabled
   Handshake secure is disabled
   802.1X unicast-trigger is enabled
   Periodic reauthentication is disabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   802.1X Multicast-trigger is enabled
   Mandatory authentication domain: NOT configured
   Guest VLAN: NOT configured
   Auth-Fail VLAN: NOT configured
   Critical VLAN: NOT configured
   Critical recovery-action: NOT configured
   Max number of on-line users is 256

   EAPOL Packet: Tx 16331, Rx 102
   Sent EAP Request/Identity Packets : 16316
        EAP Request/Challenge Packets: 6
        EAP Success Packets: 4, Fail Packets: 5
   Received EAPOL Start Packets : 6
            EAPOL LogOff Packets: 2
            EAP Response/Identity Packets : 80
            EAP Response/Challenge Packets: 6
            Error Packets: 0
 1. Authenticated user : MAC address: 0002-0000-0011

   Controlled User(s) amount to 1
```

In addition, the port allows an additional user whose MAC address has an OUI among the specified OUIs to access the port.

# Display MAC address information for interface GigabitEthernet 1/0/1.

```
<Device> display mac-address interface gigabitethernet 1/0/1
MAC ADDR        VLAN ID   STATE          PORT INDEX                AGING TIME(s)
1234-0300-0011  1         Learned        GigabitEthernet1/0/1      AGING

  ---  1 mac address(es) found  ---
```

Configuring the macAddressElseUserLoginSecure mode

Network requirements

As shown in Figure 43, 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.

Restrict port GigabitEthernet 1/0/1 of the Device:

- 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 MAC-based user accounts for MAC authentication users. The MAC addresses are hyphen separated and in lower case.
- Set the total number of MAC authenticated users and 802.1X authenticated users to 64.
- Enable NTK to prevent frames from being sent to unknown MAC addresses.

Configuration procedure

Configurations on the host and RADIUS servers are not shown.

1. Configure the RADIUS protocol:

   Configure the RADIUS authentication/accounting and ISP domain settings the same as in "Configuring the userLoginWithOUI mode."

2. Configure port security:

   # Enable port security.

   ```
   <Device> system-view
   [Device] port-security enable
   ```

   # Configure the device to use hyphenated, lowercased MAC addresses of users as the usernames and passwords for MAC authentication.

   ```
   [Device] mac-authentication user-name-format mac-address with-hyphen lowercase
   [Device] interface gigabitethernet 1/0/1
   ```

   # Specify ISP domain **sun** for MAC authentication.

   ```
   [Device] mac-authentication domain sun
   [Device] interface gigabitethernet 1/0/1
   ```

   # Set the 802.1X authentication method to CHAP. (This configuration is optional. By default, the authentication method is CHAP for 802.1X.)

   ```
   [Device] dot1x authentication-method chap
   ```

   # Set port security's limit on the number of MAC addresses to 64 on the port.

   ```
   [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
   ```

Verifying the configuration

# Display the port security configuration.

```
<Device> display port-security interface gigabitethernet 1/0/1
 Equipment port-security is enabled
 Trap is disabled
 Disableport Timeout: 20s
 OUI value:

 GigabitEthernet1/0/1 is link-up
   Port mode is macAddressElseUserLoginSecure
   NeedToKnow mode is NeedToKnowOnly
   Intrusion Protection mode is NoAction
   Max MAC address number is 64
```

```
   Stored MAC address number is 0
   Authorization is permitted
   Security MAC address learning mode is sticky
   Security MAC address aging type is absolute
```

# Display MAC authentication information.

```
<Device> display mac-authentication interface gigabitethernet 1/0/1
MAC address authentication is enabled.
User name format is MAC address in lowercase,like xx-xx-xx-xx-xx-xx
 Fixed username: mac
 Fixed password: not configured
          Offline detect period is 60s
          Quiet period is 5s
          Server response timeout value is 100s
          The max allowed user number is 1024 per slot
          Current user number amounts to 3
          Current domain is mac

Silent MAC User info:
          MAC Addr         From Port                    Port Index

GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 3, failed: 7
 Max number of on-line users is 256
  Current online user number is 3
    MAC ADDR         Authenticate state           Auth Index
    1234-0300-0011   MAC_AUTHENTICATOR_SUCCESS     13
    1234-0300-0012   MAC_AUTHENTICATOR_SUCCESS     14
    1234-0300-0013   MAC_AUTHENTICATOR_SUCCESS     15
```

# Display 802.1X authentication information.

```
<Device> display dot1x interface gigabitethernet 1/0/1
 Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 EAD quick deploy is disabled

 Configuration: Transmit Period   30 s,  Handshake Period       15 s
                Quiet Period      60 s,  Quiet Period Timer is disabled
                Supp Timeout      30 s,  Server Timeout        100 s
                The maximal retransmitting times    2
 EAD quick deploy configuration:
                EAD timeout:    30m

 Total maximum 802.1X user resource number is 1024 per slot
 Total current used 802.1X resource number is 1

GigabitEthernet1/0/1  is link-up
```

```
   802.1X protocol is enabled
   Handshake is enabled
   Handshake secure is disabled
   802.1X unicast-trigger is enabled
   Periodic reauthentication is disabled
   The port is an authenticator
   Authentication Mode is Auto
   Port Control Type is Mac-based
   802.1X Multicast-trigger is enabled
   Mandatory authentication domain: NOT configured
   Guest VLAN: NOT configured
   Auth-Fail VLAN: NOT configured
   Critical VLAN: NOT configured
   Critical recovery-action: NOT configured
   Max number of on-line users is 256

   EAPOL Packet: Tx 16331, Rx 102
   Sent EAP Request/Identity Packets : 16316
        EAP Request/Challenge Packets: 6
        EAP Success Packets: 4, Fail Packets: 5
   Received EAPOL Start Packets : 6
            EAPOL LogOff Packets: 2
            EAP Response/Identity Packets : 80
            EAP Response/Challenge Packets: 6
            Error Packets: 0
 1. Authenticated user : MAC address: 0002-0000-0011

   Controlled User(s) amount to 1
```

As NTK is enabled, frames with unknown destination MAC addresses, multicast addresses, and broadcast addresses will be discarded.

Troubleshooting port security

Cannot set the port security mode

Symptom

Cannot set the port security mode.

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
 Error:When we change port-mode, we should first change it to noRestrictions, then change
it to the other.
```

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 directly.

Solution

Set the port security mode to noRestrictions first.

```
[Device-GigabitEthernet1/0/1] undo port-security port-mode
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Cannot configure secure MAC addresses

Symptom

Cannot configure secure MAC addresses.

```
[Device-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
Error: Security MAC address configuration failed.
```

Analysis

No secure MAC address can be configured on a port operating in a port security mode other than autoLearn.

Solution

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
```

Cannot change port security mode when a user is online

Symptom

Port security mode cannot be changed when an 802.1X authenticated or MAC authenticated user is online.

```
[DeviceGigabitEthernet1/0/1] undo port-security port-mode
 Error:Cannot configure port-security for there is 802.1X user(s) on line on port
GigabitEthernet1/0/1.
```

Analysis

Changing port security mode is not allowed when an 802.1X authenticated or MAC authenticated user is online.

Solution

Use the **cut** command to forcibly disconnect the user from the port before changing the port security mode.

```
[Device-GigabitEthernet1/0/1] quit
[Device] cut connection interface gigabitethernet 1/0/1
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] undo port-security port-mode
```

Configuring a user profile

Overview

A user profile provides a configuration template to save predefined configurations, such as a Quality of Service (QoS) policy.

The user profile implements service applications on a per-user basis. Every time a user accesses the device, the device automatically applies the configurations in the user profile that is associated only with this user.

User-based traffic policing is more flexible than interface-based traffic policing. In interface-based traffic policing, if a user moves between ports to access a device, you must remove the policy from the previous port and then configure the same policy on the port being used to restrict user behaviors. The configuration task is tedious and error prone.

The user profile supports working with 802.1X and portal authentications and restricts authenticated users' behaviors as follows:

1. After the authentication server verifies a user, the server sends the device the name of the user profile associated with the user.
    - If the profile is enabled, the device applies the configurations in the user profile, and allows user access based on all valid configurations.
    - If the user profile is disabled, the device denies the user access.
2. After the user logs out, the device automatically disables the configurations in the user profile, and the restrictions on the user access are removed.

User profile configuration task list

Task	Remarks
Creating a user profile	Required
Applying a QoS policy	Required
Enabling a user profile	Required

Creating a user profile

Before you create a user profile, complete the following tasks:

- Configure authentication parameters on the device.
- Perform configurations on the client, the device, and the authentication server, for example, username, password, authentication scheme, domain, and binding a user profile with a user.

To create a user profile:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a user profile, and enter its view.	**user-profile** *profile-name*	You can use the command to enter the view of an existing user profile.

Applying a QoS policy

You can apply QoS policies in user profile view to implement traffic management functions.

Follow these guidelines when you apply a QoS policy:

- After a user profile is created, apply a QoS policy in user profile view to implement restrictions on online users. The QoS policy takes effect when the user profile is enabled and a user using the user profile goes online.
- The QoS policies that can be applied to user profiles support only the **remark**, **car**, and **filter** actions.
- Do not apply an empty policy in user profile view because a user profile with an empty policy applied cannot be enabled.
- If a user profile is enabled, you cannot modify the applied QoS policy (including the ACL that is referenced by the QoS policy) or remove it.
- For information about QoS policy configurations, see *ACL and QoS Configuration Guide*.

To apply a QoS policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter user profile view.	**user-profile** *profile-name*	N/A
3. Apply a QoS policy.	**qos apply policy** *policy-name* { **inbound** | **outbound** }	The **inbound** keyword applies the QoS policy to incoming traffic of the switch (traffic sent by online users). The **outbound** keyword applies the QoS policy to outgoing traffic of the switch (traffic sent to online users).

Enabling a user profile

Enable a user profile so that configurations in the profile can be applied by the device to restrict user behaviors. If the device detects that the user profile is disabled, the device denies the associated user even the user has been verified by the authentication server.

You can only edit or remove the configurations in a disabled user profile.

Disabling a user profile logs out the users that are using the user profile.

To enable a user profile:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable a user profile.	**user-profile** *profile-name* **enable**	A user profile is disabled by default.

Displaying and maintaining user profiles

Task	Command	Remarks
Display information about all the created user profiles.	**display user-profile** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Configuring password control

Overview

Password control refers to a set of functions provided by the local authentication server to control user login passwords, super passwords, and user login status based on predefined policies. The rest of this section describes the password control functions in detail.

- Minimum password length

  By setting a minimum password length, you can enforce users to use passwords long enough for system security. If a user specifies a shorter password, the system rejects the setting and prompts the user to re-specify a password.

- Minimum password update interval

  This function allows you to set the minimum interval at which users can change their passwords. If a non-manage level user logs in to change the password but the time that elapses 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 non-manage level user cannot change the password twice within 48 hours. This prevents users from changing their passwords frequently.

NOTE:

- This function is not effective on users of the manage level. For information about user levels, see *Fundamentals Configuration Guide*.
- This function is not effective on a user who is prompted to change the password at the first login or a user whose password has just been aged out.

- Password aging

  Password aging imposes a lifecycle on a user password. After the password aging time expires, the user needs to change the password.

  If a user enters an expired password when logging in, the system displays an error message and prompts the user to provide a new password and to confirm it by entering it again. The new password must be a valid one and the user must enter exactly the same password when confirming it.

- 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 period. If so, the system notifies the user of the expiration time and provides a choice for the user to change the password. If the user provides a new password that is complexity-compliant, the system records the new password and the time. If the user chooses to leave the password or the user fails to change it, the system allows the user to log in using the current password.

NOTE:

Telnet, SSH, and terminal users can change their passwords by themselves, while FTP users can only have their passwords changed by the administrator.

- 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, so that the user does not need to change the password immediately. For example, if you set the maximum number of logins with an expired password to three 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 maintains certain entries of passwords that a user has used. When a user changes the password, the system checks the new password against the history passwords and the current password. The new password must be different from the used ones by at least four characters and the four characters must not be the same. Otherwise, the user will fail to change the password and the system displays an error message.

  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 latest record will overwrite the earliest one.

- Login attempt limit

  Limiting the number of consecutive failed login attempts can effectively prevent password guessing.

  If an FTP or virtual terminal line (VTY) user fails authentication due to a password error, the system adds the user to a password control blacklist. If a user fails to provide the correct password after the specified number of consecutive attempts, the system takes action as configured:

  - Prohibiting the user from logging in until the user is removed from the password control blacklist manually.
  - Allowing the user to try continuously and removing the user from the password control blacklist when the user logs in to the system successfully or the blacklist entry times out (the blacklist entry aging time is one minute).
  - Prohibiting the user from logging in within a configurable period of time, and allowing the user to log in again after the period of time elapses or the user is removed from the password control blacklist.

  A password control blacklist can contain up to 1024 entries.

  A login attempt using a wrong username will undoubtedly fail but the username will not be added to the password control blacklist.

  Users accessing the system through the console interface are not blacklisted, because the system is unable to obtain the IP addresses of these users and these users are privileged and therefore relatively secure to the system.

- Password composition checking

  A password can be a combination of characters from the following four types:

  - Uppercase letters A to Z
  - Lowercase letters a to z
  - Digits 0 to 9
  - 32 special characters: blank space, tilde (~), back quote (`), exclamation point (!), at sign (@), pound sign (#), dollar sign ($), percent sign (%), caret (^), ampersand sign (&), asterisk (*), left parenthesis ("("), right parenthesis (")"), underscore (_), plus sign (+), minus sign (-), equal sign (=), left brace ({), right brace (}), vertical bar (|), left bracket ([), right bracket (]), back slash (\), colon (:), quotation marks ("), semi-colon (;), apostrophe ('), left angle bracket (<), right angle bracket (>), comma (,), dot (.), and slash (/)

Depending on the system security requirements, you can set the minimum number of character types a password must contain and the minimum number of characters that are from each type in the password.

There are four password combination levels in non-FIPS mode: 1, 2, 3, and 4, each representing the number of character types that a password must at least contain. Level 1 means that a password must contain characters of one type, level 2 at least two types, and so on.

In FIPS mode, a password must contain four types of characters and each type contains at least one character.

When a user sets or changes the password, the system checks if the password meets the composition requirement. If not, the system displays an error message.

- Password complexity checking

  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 that 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 system refuses the password and displays a password configuration failure message.

  You can impose 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 weak.
  - No character of the password is repeated three or more times consecutively. For example, password a111 is weak.

- Password display in the form of a string of asterisks (*)

  For the sake of security, the password a user enters is displayed in the form of a string of asterisks (*).

- Authentication timeout management

  The authentication period is from when the server obtains the username to when the server finishes authenticating the user's password. If a Telnet user fails to log in within the configured period of time, the system tears down the connection.

- Maximum account idle time

  You can set the maximum account idle time to make accounts staying idle for this period of time become invalid and unable to log in again. For example, if you set the maximum account idle time to 60 days and user using the account **test** has never logged in successfully within 60 days after the last successful login, the account becomes invalid.

- Logging

  The system logs all successful password changing events and the events of adding users 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 functions can be configured in several views, and different views support different functions. The settings configured in different views or for different objects have different application ranges and different priorities:

- Global settings in system view apply to all local user passwords and super passwords.
- Settings in user group view apply to the passwords of all local users in the user group.
- Settings in local user view apply to only the password of the local user.
- Settings for super passwords apply to only super passwords.

The above four types of settings have different priorities:

- For local user passwords, the settings with a smaller application range have a higher priority.
- For super passwords, the settings configured specifically for super passwords, if any, override those configured in system view.

Complete the following tasks to configure password control:

Task	Remarks
Enabling password control	Required
Setting global password control parameters	Optional
Setting user group password control parameters	Optional
Setting local user password control parameters	Optional
Setting super password control parameters	Optional
Setting a local user password in interactive mode	Optional

Configuring password control

Enabling password control

To enable password control functions, you need to:

1. Enable the password control feature in system view. Password control configurations take effect only after the password control feature is enabled globally.
2. Enable a specific password control function. The following password control functions need to be enabled individually after the password control feature is enabled globally:
    - Password aging
    - Minimum password length
    - Password history
    - Password composition checking

You must enable a function for its relevant configurations to take effect.

To enable password control:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the password control feature.	**password-control enable**	Disabled by default.
3.	Enable a password control function individually.	**password-control** { **aging** | **composition** | **history** | **length** } **enable**	Optional. All of the four password control functions are enabled by default.

After global password control is enabled, local user passwords configured on the device are not displayed when you use the corresponding **display** command.

For security purposes, the system prompts the Telnet, SSH, and terminal users to change their passwords the first time they log in to the device after the global password control is enabled. Because FTP users can only have their passwords changed by the administrator, if the administrator does not change passwords for the FTP users after the global password control is enabled, the FTP users cannot log in to the device.

About the minimum password length:

- When global password control is disabled, the minimum password length is one character.
- When global password control is enabled but the minimum password length restriction function and FIPS mode are disabled, the minimum password length is four characters, and the password must have at least four different characters.
- When global password control and FIPS mode are enabled but the minimum password length restriction function is disabled, the minimum password length is eight characters, and the password must have at least four different characters.
- When global password control and the minimum password length restriction function are both enabled, the minimum password length is that configured by the **password-control length** *length* command. However, the password must meet the FIPS requirements.

About password history control:

- When global password control is disabled, or when global password control is enabled but the password history control is disabled, the device does not record history passwords and allows a user to set a new password the same as a previously used one.
- When global password control and password history control are both enabled, the system records history passwords for users. When a user changes the password, the system compares the new password against the history passwords and the current password. The new password must be different from the used ones by at least four characters and the four characters must not be the same. Otherwise, the user will fail to change the password.

Setting global password control parameters

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the password aging time.	**password-control aging** *aging-time*	Optional. 90 days by default.
3.	Set the minimum password update interval.	**password-control password update interval** *interval*	Optional. 24 hours by default.

Step	Command	Remarks
4. Set the minimum password length.	**password-control length** *length*	Optional. 10 characters by default.
5. Configure the password composition policy.	**password-control composition type-number** *type-number* [**type-length** *type-length*]	Optional. • In non-FIPS mode, by default, a password must contain at least one type of characters and each type must contain at least one character. • In FIPS mode, by default, a password must contain four types of characters and each type must contain at least one character.
6. Configure the password complexity checking policy.	**password-control complexity** { **same-character** | **user-name** } **check**	Optional. By default, the system does not perform password complexity checking.
7. Set the maximum number of history password records for each user.	**password-control history** *max-record-num*	Optional. 4 by default.
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.	**password-control login-attempt** *login-times* [**exceed** { **lock** | **unlock** | **lock-time** *time* }]	Optional. By default, the maximum number of login attempts is 3 and a user failing to log in after the specified number of attempts must wait for one minute before trying again.
9. Set the number of days during which the user is warned of the pending password expiration.	**password-control alert-before-expire** *alert-time*	Optional. 7 days by default.
10. Set the maximum number of days and maximum number of times that a user can log in after the password expires.	**password-control expired-user-login delay** *delay* **times** *times*	Optional. By default, a user can log in three times within 30 days after the password expires.
11. Set the authentication timeout time.	**password-control authentication-timeout** *authentication-timeout*	Optional. 60 seconds by default.
12. Set the maximum account idle time.	**password-control login idle-time** *idle-time*	Optional. 90 days by default.

NOTE:

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 for users that have been logged in or passwords that have been configured.

Setting user group password control parameters

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a user group and enter user group view.	**user-group** *group-name*	N/A
3.	Configure the password aging time for the user group.	**password-control aging** *aging-time*	Optional By default, the aging time of the user group is the same as the global password aging time.
4.	Configure the minimum password length for the user group.	**password-control length** *length*	Optional By default, the minimum password length of the user group is the same as the global minimum password length.
5.	Configure the password composition policy for the user group.	**password-control composition type-number** *type-number* [**type-length** *type-length*]	Optional By default, the password composition policy of the user group is the same as the global password composition policy.

Setting local user password control parameters

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a local user and enter local user view.	**local-user** *user-name*	N/A
3.	Configure the password aging time for the local user.	**password-control aging** *aging-time*	Optional By default, the setting equals that for the user group to which the local user belongs. If no aging time is configured for the user group, the global setting applies to the local user.
4.	Configure the minimum password length for the local user.	**password-control length** *length*	Optional By default, the setting equals that for the user group to which the local user belongs. If no minimum password length is configured for the user group, the global setting applies to the local user.
5.	Configure the password composition policy for the local user.	**password-control composition type-number** *type-number* [**type-length** *type-length*]	Optional By default, the settings equal those for the user group to which the local user belongs. If no password composition policy is configured for the user group, the global settings apply to the local user.

Setting super password control parameters

CLI commands fall into four levels: visit, monitor, system, and manage, in ascending order. Accordingly, login users fall into four levels, each corresponding to a command level. A user of a certain level can only use the commands at that level or lower levels.

To switch from a lower user level to a higher one, a user needs to enter a password for authentication. This password is called a super password. For more information on super passwords, see *Fundamentals Configuration Guide*.

To set super password control parameters:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the password aging time for super passwords.	**password-control super aging** *aging-time*	Optional. By default, the super password aging time is the same as the global password aging time.
3. Configure the minimum length for super passwords.	**password-control super length** *length*	Optional. By default, the minimum super password length is the same as the global minimum password length.
4. Configure the password composition policy for super passwords.	**password-control super composition type-number** *type-number* [**type-length** *type-length*]	Optional. By default, the super password composition policy is the same as the global password composition policy.

Setting a local user password in interactive mode

You can set a password for a local user in interactive mode. When doing so, you need to confirm the password.

To set a password for a local user in interactive mode:

Step	Command
1. Enter system view.	**system-view**
2. Create a local user and enter local user view.	**local-user** *user-name*
3. Set the password for the local user in interactive mode.	**password**

Displaying and maintaining password control

Task	Command	Remarks
Display password control configuration information.	**display password-control** [**super**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Task	Command	Remarks
Display information about users in the password control blacklist.	**display password-control blacklist** [**user-name** *name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Delete users from the password control blacklist.	**reset password-control blacklist** [**all** | **user-name** *name*]	Available in user view
Clear history password records.	**reset password-control history-record** [**user-name** *name* | **super** [**level** *level*]]	Available in user view

NOTE:

The **reset password-control history-record** command can delete the history password records of a specific user or all users even when the password history function is disabled.

Password control configuration example

All commands in the following example are executed in non-FIPS mode.

Network requirements

Implementing the following global password control policy:

- 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.
- The password aging time is 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 occurs consecutively three or more times in a password.

Implementing the following super password control policy: A super password must contain at least three types of valid characters, five or more of each type.

Implementing the following password control policy for local Telnet user **test**:

- The password must contain at least 12 characters.
- The password must consist of at least two types of valid characters, five or more of each type.
- The password aging time is 20 days.

Configuration procedure

# Enable the password control feature globally.

```
<Sysname> system-view
[Sysname] password-control enable
```

# Prohibit the user from logging in forever after two successive login failures.

```
[Sysname] password-control login-attempt 2 exceed lock
```

# Set the password aging time to 30 days for all passwords.

```
[Sysname] password-control aging 30
```

# Set the minimum password update interval to 36 hours.

```
[Sysname] password-control password 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 of the password can be repeated three or more times consecutively.

```
[Sysname] password-control complexity same-character check
```

# Specify that a super password must contain at least three types of characters and each type must contain at least five characters.

```
[Sysname] password-control super composition type-number 3 type-length 5
```

# Configure a super password.

```
[Sysname] super password level 3 simple 12345ABGFTweuix
```

# Create a local user named test.

```
[Sysname] local-user test
```

# Set the service type of the user to Telnet.

```
[Sysname-luser-test] service-type telnet
```

# Set the minimum password length to 12 for the local user.

```
[Sysname-luser-test] password-control length 12
```

# Specify that the password of the local user must contain at least two types of characters and each type must contain at least five characters.

```
[Sysname-luser-test] password-control composition type-number 2 type-length 5
```

# Set the password aging time to 20 days for the local user.

```
[Sysname-luser-test] password-control aging 20
```

# Configure the password of the local user in interactive mode.

```
[Sysname-luser-test] password
Password:***********
Confirm :***********
Updating user(s) information, please wait........
[Sysname-luser-test] quit
```

Verifying the configuration

# Display the global password control configuration information.

```
<Sysname> display password-control
Global password control configurations:
 Password control:                     Enabled
 Password aging:                       Enabled (30 days)
 Password length:                      Enabled (10 characters)
 Password composition:                 Enabled (1 types,  1 characters per type)
 Password history:                     Enabled (max history record:4)
 Early notice on password expiration: 7 days
 User authentication timeout:         60 seconds
 Maximum failed login attempts:       2 times
 Login attempt-failed action:         Lock
 Minimum password update time:        36 hours
 User account idle-time:              30 days
 Login with aged password:            5 times in 60 day(s)
 Password complexity:                 Enabled (username checking)
                                      Enabled (repeated characters checking)
```

# Display the password control configuration information for super passwords.

```
<Sysname> display password-control super
 Super password control configurations:
 Password aging:                      Enabled (30 days)
 Password length:                     Enabled (10 characters)
 Password composition:                Enabled (3 types,  5 characters per type)
```

# Display the password control configuration information for local user **test**.

```
<Sysname> display local-user user-name test
The contents of local user test:
 State:                    Active
 ServiceType:              telnet
 Access-limit:             Disable           Current AccessNum: 0
 User-group:               system
 Bind attributes:
 Authorization attributes:
 Password aging:                       Enabled (20 days)
 Password length:                      Enabled (12 characters)
 Password composition:                 Enabled (2 types,  5 characters per type)
Total 1 local user(s) matched.
```

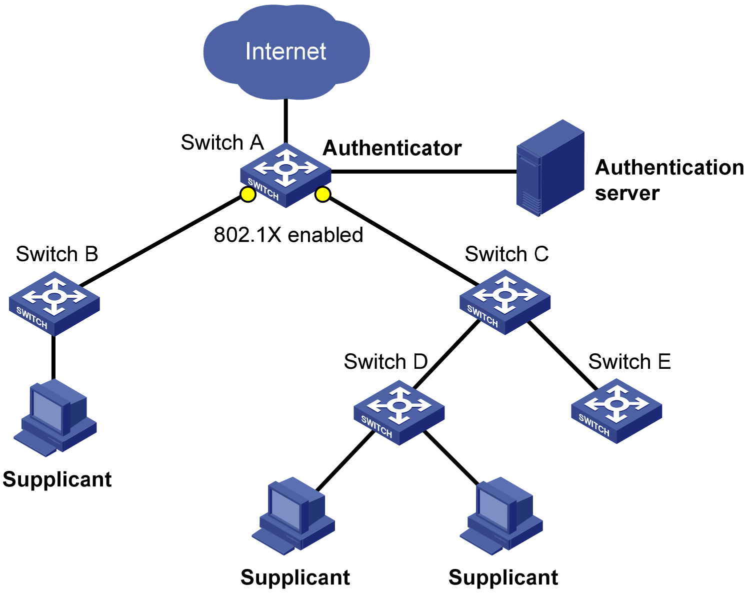
Configuring HABP

Overview

The HW Authentication Bypass Protocol (HABP) is intended to enable the downstream network devices of an access device to bypass 802.1X authentication and MAC authentication configured on the access device.

As shown in Figure 44, 802.1X authenticator Switch A has two switches attached to it: Switch B and Switch C. On Switch A, 802.1X authentication is enabled globally and on the ports connecting the downstream network devices. The end-user devices (the supplicants) run the 802.1X client software for 802.1X authentication. For Switch B and Switch D, where the 802.1X client is not supported (which is typical of network devices), the communication between them will fail because they cannot pass 802.1X authentication and their packets will be blocked on Switch A. To allow the two switches to communicate, you can use HABP.

Figure 44 Network diagram for HABP application



HABP is a link layer protocol that works above the MAC layer. It is built on the client-server model. Generally, the HABP server is enabled on the authentication device (which is configured with 802.1X or MAC authentication, such as Switch A in the above example), and the attached switches function as the HABP clients, such as Switch B through Switch E in the example. No device can function as both an HABP server and a client at the same time. Typically, the HABP server sends HABP requests to all its clients periodically to collect their MAC addresses, and the clients respond to the requests. After the server learns the MAC addresses of all the clients, it registers the MAC addresses as HABP entries. Then, link layer frames exchanged between the clients can bypass the 802.1X authentication on ports of the server without affecting the normal operation of the whole network. All HABP packets must travel in a specified VLAN. Communication between the HABP server and HABP clients is implemented through this VLAN.

In a cluster, if a member switch with 802.1X authentication or MAC authentication enabled is attached with some other member switches of the cluster, you also need to configure HABP server on this device.

Otherwise, the cluster management device will not be able to manage the devices attached to this member switch. For more information about the cluster function, see *Network Management and Monitoring Configuration Guide*.

Configuring HABP

Configuring the HABP server

An HABP server is usually configured on the authentication device enabled with 802.1X authentication or MAC address authentication. The HABP server sends HABP requests to the attached switches (HABP clients) at a specified interval, collecting their MAC addresses from the responses. HABP packets are transmitted in the VLAN specified on the HABP server.

To configure an HABP server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable HABP.	**habp enable**	Optional Enabled by default
3. Configure HABP to work in server mode and specify the VLAN for HABP packets.	**habp server vlan** *vlan-id*	HABP works in client mode by default. The VLAN specified on the HABP server for transmitting HABP packets must be the same as that to which the HABP clients belong.
4. Set the interval to send HABP requests.	**habp timer** *interval*	Optional 20 seconds by default

Configuring an HABP client

An HABP client is usually configured on each device that is attached to the authentication device. After receiving an HABP request from the HABP server, an HABP client responds to the request, delivering its MAC address to the server, and forwards the HABP request to its attached switches. HABP packets are transmitted in the VLAN to which the HABP client belongs.

To configure an HABP client:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable HABP.	**habp enable**	Optional Enabled by default
3. Configure HABP to work in client mode.	**undo habp server**	Optional HABP works in client mode by default.

Step	Command	Remarks
4. Specify the VLAN to which the HABP client belongs.	**habp client vlan** *vlan-id*	Optional By default, an HABP client belongs to VLAN 1. The VLAN to which an HABP client belongs must be the same as that specified on the HABP server for transmitting HABP packets.

Displaying and maintaining HABP

Task	Command	Remarks
Display HABP configuration information.	**display habp** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display HABP MAC address table entries.	**display habp table** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display HABP packet statistics.	**display habp traffic** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

HABP configuration example

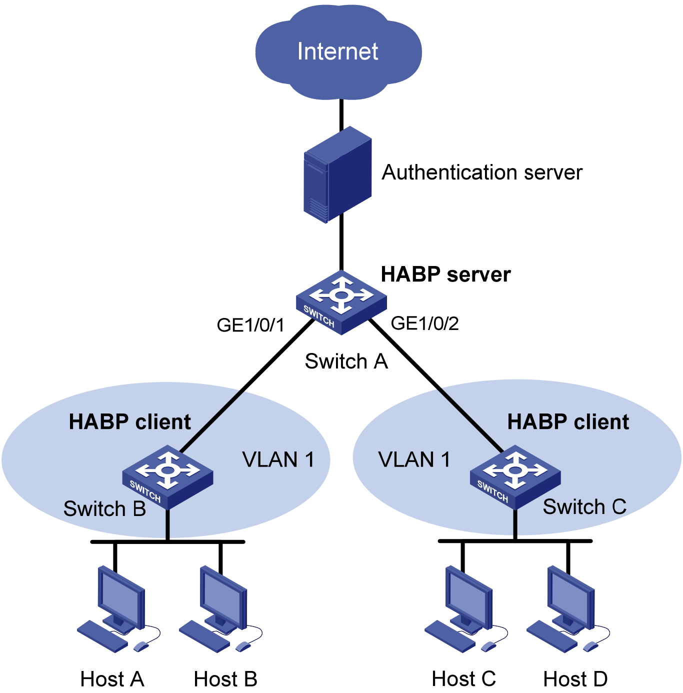
Network requirements

As shown in Figure 45, Switch A is attached with access devices Switch B and Switch C. 802.1X authentication is configured on Switch A for central authentication and management of users (Host A through Host D).

For communication between Switch B and Switch C, enable HABP server on Switch A, enable HABP client on Switch B and Switch C, and specify VLAN 1 for HABP packets.

Configure the HABP server to send HABP request packets to the HABP clients in VLAN 1 at an interval of 50 seconds.

Figure 45 Network diagram



Configuration procedure

1. Configure Switch A:

   # Perform 802.1X related configurations on Switch A (see "Configuring 802.1X").

   # Enable HABP. (HABP is enabled by default. This configuration is optional.)

```
<SwitchA> system-view
[SwitchA] habp enable
```

   # Configure HABP to work in server mode, and specify VLAN 1 for HABP packets.

```
[SwitchA] habp server vlan 1
```

   # Set the interval at which the switch sends HABP request packets to 50 seconds.

```
[SwitchA] habp timer 50
```

2. Configure Switch B:

   # Enable HABP. (HABP is enabled by default. This configuration is optional.)

```
<SwitchA> system-view
[SwitchB] habp enable
```

   # Configure HABP to work in client mode. (HABP works in client mode by default. This configuration is optional.)

```
[SwitchB] undo habp server
```

   # Specify the VLAN to which the HABP client belongs as VLAN 1. (An HABP client belongs to VLAN 1 by default. This configuration is optional.)

```
[SwitchB] habp client vlan 1
```

3. Configure Switch C:

   Configurations on Switch C are similar to those on Switch B.

4. Verify your configuration:

   # Display HABP configuration information.

```
<SwitchA> display habp
Global HABP information:
         HABP Mode: Server
         Sending HABP request packets every 50 seconds
         Bypass VLAN: 1
```

# Display HABP MAC address table entries.

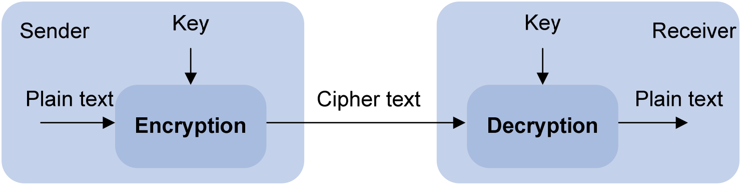
```
<SwitchA> display habp table
MAC             Holdtime  Receive Port
001f-3c00-0030  53        GigabitEthernet1/0/2
001f-3c00-0031  53        GigabitEthernet1/0/1
```

Managing public keys

Overview

To protect data confidentiality during transmission, the data sender uses an algorithm and a key (a character string) to encrypt the plain text data before sending the data out, and the receiver uses the same algorithm with the help of a key to decrypt the data, as shown in Figure 46.

Figure 46 Encryption and decryption



The keys that participate in the conversion between the plain text and the cipher text can be the same or different, dividing the encryption and decryption algorithms into the following types:

- **Symmetric key algorithm**—The keys for encryption and decryption are the same.
- **Asymmetric key algorithm**—The keys for encryption and decryption are different, one is the public key, and the other is the private key. The information encrypted with the public key can only be decrypted with the corresponding private key, and vice versa. The private key is kept secret, and the public key may be distributed widely. The private key cannot be practically derived from the public key. Asymmetric key algorithms include the Revest-Shamir-Adleman Algorithm (RSA), and the Digital Signature Algorithm (DSA).

Asymmetric key algorithms can be used in two scenarios for two purposes:

- **To encrypt and decrypt data**—The sender uses the public key of the intended receiver to encrypt the information to be sent. Only the intended receiver, the holder of the paired private key, can decrypt the information. This mechanism guarantees confidentiality. Only RSA can be used for data encryption and decryption.
- **To authenticate a sender**—This application is called digital signature. The sender "signs" the information to be sent by encrypting the information with its own private key. A receiver decrypts the information with the sender's public key and, based on whether the information can be decrypted, determines the authenticity of the information. RSA and DSA can be used for digital signature.

Asymmetric key algorithms are widely used in various applications. For example, Secure Shell (SSH), Secure Sockets Layer (SSL), and Public Key Infrastructure (PKI) use the algorithms for digital signature. For information about SSH, SSL, and PKI, see "Configuring SSH2.0," "Configuring SSL," and "Configuring PKI."

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.

Configuration task list

Public key configuration tasks enable you to manage the local asymmetric key pairs, and configure the peer host public keys on the local device. By completing these tasks, the local device is ready to work with applications such as SSH and SSL to implement data encryption/decryption, or digital signature.

Complete these tasks to configure public keys:

Task		Remarks
Configuring a local asymmetric key pair on the local device.	Creating a local asymmetric key pair	Perform the tasks as needed.
	Displaying or exporting the local host public key	
	Destroying a local asymmetric key pair	
Specifying the peer public key on the local device		

Creating a local asymmetric key pair

When you create an asymmetric key pair on the local device, follow these guidelines:

- Create an asymmetric key pair of the proper type to work with a target application.
- After you enter the command, specify a proper modulus length for the key pair. The following table compares the three types of key pairs.

Type	Number of key pairs	Modulus length	Remarks
RSA (in non-FIPS mode)	Two key pairs, one server key pair and one host key par. Each key pair comprises a public key and a private key.	512 to 2048 bits. 1024 by default.	To achieve high security, specify at least 768 bits.
RSA (in FIPS mode)	One key pair, the host key pair.	2048 bits.	N/A
DSA (in non-FIPS mode)	One key pair, the host key pair.	512 to 2048 bits. 1024 by default.	To achieve high security, specify at least 768 bits.
DSA (in FIPS mode)	One key pair, the host key pair.	1024 to 2048 bits. 1024 by default.	N/A

To create a local asymmetric key pair:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a local asymmetric key pair.	**public-key local create** { **dsa** | **rsa** }	By default, no asymmetric key pair is created. Key pairs created with the **public-key local create** command are saved automatically and can survive system reboots.

Displaying or exporting the local host public key

In some applications, such as SSH, to allow your local device to be authenticated by a peer device through digital signature, you must display or export the local host public key, which will then be specified on the peer device.

To display or export the local host public key, choose one of the following methods:

- Displaying and recording the host public key information
- Displaying the host public key in a specific format and saving it to a file
- Exporting the host public key in a specific format to a file

If your local device functions to authenticate the peer device, you must specify the peer public key on the local device. For more information, see "Specifying the peer public key on the local device."

Displaying and recording the host public key information

To display the local public key:

Task	Command	Remarks
Display the local RSA public keys.	**display public-key local rsa public** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view. Use at least one command.
Display the local host public key.	**display public-key local dsa public** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	

The **display public-key local rsa public** command displays both the RSA server and host public keys. Recording the RSA host public key is enough.

After displaying the host public key, record the key information for manual configuration of the key on the peer device.

Displaying the host public key in a specific format and saving it to a file

To display the local host public key in a specific format:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Display the local RSA or DSA host public key in a specific format.	• To display the local RSA host public key: ○ In non-FIPS mode: **public-key local export rsa** { **openssh** | **ssh1** | **ssh2** } ○ In FIPS mode: **public-key local export rsa** { **openssh** | **ssh2** } • To display the local DSA host public key: **public-key local export dsa** { **openssh** | **ssh2** }	Use at least one command.

After you display the host public key in a specify format, save the key to a file (by using a method such as copying and-pasting), and transfer this file to the peer device.

Exporting the host public key in a specific format to a file

After you export and save the host public key in a specify format to a file, transfer the file to the peer device.

To export and save the local host public key to a file:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Export a local RSA or DSA host public key in a specific format to a file.	• To export a local RSA host public key: ○ In non-FIPS mode: **public-key local export rsa** { **openssh** | **ssh1** | **ssh2** } *filename* ○ In FIPS mode: **public-key local export rsa** { **openssh** | **ssh2** } *filename* • To export a local DSA host public key: **public-key local export dsa** { **openssh** | **ssh2** } *filename*	Use at least one command.

Destroying a local asymmetric key pair

You may need to destroy a local asymmetric key pair and generate a new pair when an intrusion event has occurred, the storage media of the device is replaced, the asymmetric key has been used for a long time, or the local certificate expires. For more information about the local certificate, see "Configuring PKI."

To destroy a local asymmetric key pair:

Step	Command
1. Enter system view.	**system-view**
2. Destroy a local asymmetric key pair.	**public-key local destroy** { **dsa** | **rsa** }

Specifying the peer public key on the local device

In some applications, such as SSH, to enable the local device to authenticate a peer device, specify the peer public key on the local device. The device supports up to 20 peer public keys.

For information about displaying or exporting the host public key, see "Displaying or exporting the local host public key."

Take one of the following methods to specify the peer public key on the local device:

Method	Prerequisites	Remarks
Import the public key from a public key file (recommended).	3. Save the host public key of the intended asymmetric key pair in a file. 4. Transfer a copy of the file through FTP or TFTP in binary mode to the local device.	During the import process, the system automatically converts the public key to a string in Public Key Cryptography Standards (PKCS) format.
Manually configure the public key—enter or copy the key data.	• Display and record the public key of the intended asymmetric key pair. • If the peer device is an HP device, use the **display public-key local public** command to view and record its public key. A public key displayed by other methods for the HP device might not be in a correct format.	• The recorded public key must be in the correct format. Otherwise, the manual configuration of a format-incompliant public key will fail. • Always use the first method if you are not sure about the format of the recorded public key.

To import the host public key from a public key file to the local device:

Step	Command
1. Enter system view.	**system-view**
2. Import the host public key from the public key file.	**public-key peer** *keyname* **import sshkey** *filename*

To manually configure the peer public key on the local device:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify a name for the public key and enter public key view.	**public-key peer** *keyname*	N/A
3. Enter public key code view.	**public-key-code begin**	N/A
4. Configure the peer public key.	Enter or copy the key	Spaces and carriage returns are allowed between characters, but are not saved.
5. Return to public key view.	**public-key-code end**	When you exit public key code view, the system automatically saves the public key.
6. Return to system view.	**peer-public-key end**	N/A

Displaying and maintaining public keys

Task	Command	Remarks
Display the local public keys.	**display public-key local** { **dsa** | **rsa** } **public** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the specified or all peer public keys on the local device.	**display public-key peer** [**brief** | **name** *publickey-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Public key configuration examples

Unless otherwise noted, devices in the configuration examples are operating in non-FIPS mode.

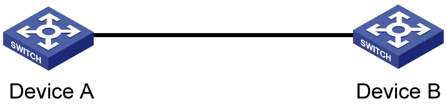
Manually specifying the peer public key on the local device

Network requirements

As shown in Figure 47, to prevent illegal access, Device B (the local device) authenticates Device A (the peer device) 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.
- Manually specify the host public key of Device A's public key pair on Device B.

Figure 47 Network diagram



Configuration procedure

1. Configure Device A;

   # Create local RSA key pairs on Device A, setting the modulus length to the default, 1024 bits.

```
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++
++++++
++++++++
++++++++
```

   # Display the public keys of the local RSA key pairs.

```
[DeviceA] display public-key local rsa public

=====================================================
Time of Key pair created: 09:50:06  2012/03/07
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F
814F9854C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E7
66BD995C669A784AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA32647
0034DC078B2BAA3BC3BCA80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001

=====================================================
Time of Key pair created: 09:50:07  2012/03/07
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100999089E7AEE9802002D9EB2D0433B87
BB6158E35000AFB3FF310E42F109829D65BF70F7712507BE1A3E0BC5C2C03FAAF00DFDDC63D004B44
90DACBA3CFA9E84B9151BDC7EECE1C8770D961557D192DE2B36CAF9974B7B293363BB372771C2C1F0
203010001
```

2. Configure Device B:

   # Configure the host public key of Device A's RSA key pairs on Device B. In public key code view, input the host public key of Device A. The host public key is the content of HOST_KEY displayed on Device A by using the **display public-key local dsa public** command.

   ```
   <DeviceB> system-view
   [DeviceB] public-key peer devicea
   Public key view: return to System View with "peer-public-key end".
   [DeviceB-pkey-public-key] public-key-code begin
   Public key code view: return to last view with "public-key-code end".
   [DeviceB-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100
   D90003FA95F5A44A2A2CD3F814F9854C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6
   E5E51E5E353B3A9AB16C9E766BD995C669A784AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994
   E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA80AAB5EE01986BD1EF64B42F17CCAE4A77F1E
   F999B2BF9C4A10203010001
   [DeviceB-pkey-key-code] public-key-code end
   [DeviceB-pkey-public-key] peer-public-key end
   ```

   # Display the host public key of Device A saved on Device B.

   ```
   [DeviceB] display public-key peer name devicea

   =====================================
     Key Name  : devicea
     Key Type  : RSA
     Key Module: 1024
   =====================================
   Key Code:
   30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F
   814F9854C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E7
   66BD995C669A784AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA32647
   0034DC078B2BAA3BC3BCA80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
   ```

The output shows that the host public key of Device A saved on Device B is consistent with the one created on Device A.

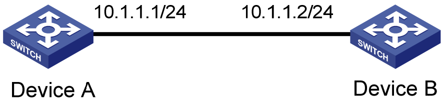
Importing a peer public key from a public key file

Network requirements

As shown in Figure 48, to prevent illegal access, Device B (the local device) authenticates Device A (the peer device) 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.
- Import the host public key of Device A from the public key file to Device B.

Figure 48 Network diagram



Configuration procedure

1. Create key pairs on Device A and export the host public key:

   # Create local RSA key pairs on Device A, setting the modulus length to the default, 1024 bits.

```
<DeviceA> system-view
[DeviceA] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++
++++++
++++++++
++++++++
```

   # Display the public keys of the local RSA key pairs.

```
[DeviceA] display public-key local rsa public

=====================================================
Time of Key pair created: 09:50:06  2012/03/07
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F
814F9854C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E7
66BD995C669A784AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA32647
0034DC078B2BAA3BC3BCA80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001

=====================================================
Time of Key pair created: 09:50:07  2012/03/07
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100999089E7AEE9802002D9EB2D0433B87
BB6158E35000AFB3FF310E42F109829D65BF70F7712507BE1A3E0BC5C2C03FAAF00DFDDC63D004B44
90DACBA3CFA9E84B9151BDC7EECE1C8770D961557D192DE2B36CAF9974B7B293363BB372771C2C1F0
203010001
```

# Export the RSA host public key HOST_KEY to a file named **devicea.pub**.

```
[DeviceA] public-key local export rsa ssh2 devicea.pub
```

2. On Device A, enable the FTP server function, create an FTP user with the username **ftp**, password **123**, and user level **3**. This user level guarantees that the user has the permission to perform FTP operations.

```
[DeviceA] ftp server enable
[DeviceA] local-user ftp
[DeviceA-luser-ftp] password simple 123
[DeviceA-luser-ftp] service-type ftp
[DeviceA-luser-ftp] authorization-attribute level 3
[DeviceA-luser-ftp] quit
```

3. On Device B, use FTP to log in to Device A, and get the public key file **devicea.pub** with the file transfer mode of binary.

```
<DeviceB> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 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.
[ftp] binary
200 Type set to I.
[ftp] get devicea.pub
227 Entering Passive Mode (10,1,1,1,5,148).
125 BINARY mode data connection already open, transfer starting for /devicea.pub.
226 Transfer complete.
FTP: 299 byte(s) received in 0.189 second(s), 1.00Kbyte(s)/sec.
[ftp] quit
221 Server closing.
```

4. Import the host public key of Device A to Device B:

# Import the host public key of Device A from the key file **devicea.pub** to Device B.

```
<DeviceB> system-view
[DeviceB] public-key peer devicea import sshkey devicea.pub
```

# Display the host public key of Device A on Device B.

```
[DeviceB] display public-key peer name devicea

=====================================
  Key Name  : devicea
  Key Type  : RSA
  Key Module: 1024
=====================================
Key Code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F
814F9854C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E7
66BD995C669A784AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA32647
0034DC078B2BAA3BC3BCA80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

The output shows that the host public key of Device A saved on Device B is consistent with the one created on Device A.

Configuring PKI

Overview

The Public Key Infrastructure (PKI) is a general security infrastructure used to provide information security through public key technologies.

PKI, also called asymmetric key infrastructure, uses a key pair to encrypt and decrypt the data. The key pair consists of a private key and a public key. The private key must be kept secret but the public key needs to be distributed. Data encrypted by one of the two keys can only be decrypted by the other.

A key problem with PKI is how to manage the public keys. PKI employs the digital certificate mechanism to solve this problem. The digital certificate mechanism binds public keys to their owners, helping distribute public keys in large networks securely.

With digital certificates, the PKI system provides network communication and e-commerce with security services such as user authentication, data non-repudiation, data confidentiality, and data integrity.

HP's PKI system provides certificate management for Secure Sockets Layer (SSL).

PKI terms

- Digital certificate

  A digital certificate is a file signed by a certificate authority (CA) for an entity. It includes mainly the identity information of the entity, the public key of the entity, the name and signature of the CA, and the validity period of the certificate. The signature of the CA ensures the validity and authority of the certificate. A digital certificate must comply with the international standard of ITU-T X.509. The most common standard is X.509 v3.

  This document discusses two types of certificates: local certificate and CA certificate. A local certificate is a digital certificate signed by a CA for an entity. A CA certificate is the certificate of a CA. If multiple CAs are trusted by different users in a PKI system, the CAs will form a CA tree with the root CA at the top level. The root CA has a CA certificate signed by itself and each lower level CA has a CA certificate signed by the CA at the next higher level.

- CRL

  An existing certificate might need to be revoked when, for example, the username changes, the private key leaks, or the user stops the business. Revoking a certificate removes the binding of the public key with the user identity information. In PKI, the revocation is made through certificate revocation lists (CRLs). Whenever a certificate is revoked, the CA publishes one or more CRLs to show all certificates that have been revoked. The CRLs contain the serial numbers of all revoked certificates and provide an effective way for checking the validity of certificates.

  A CA might publish multiple CRLs when the number of revoked certificates is so large that publishing them in a single CRL might degrade network performance. A CA uses CRL distribution points to indicate the URLs of these CRLs.

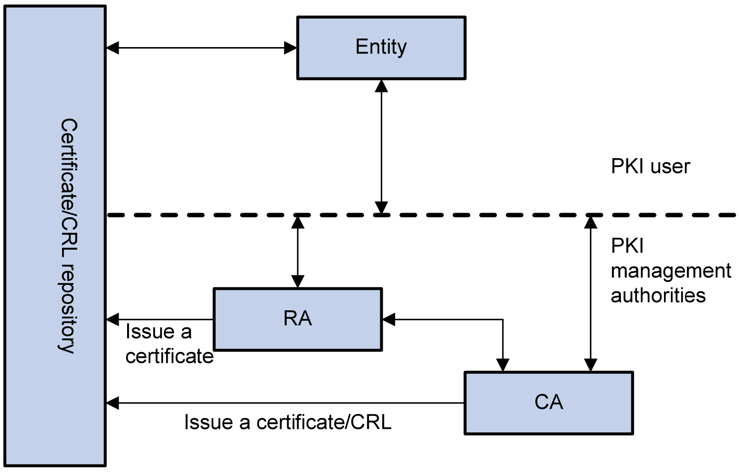
- CA policy

  A CA policy is a set of criteria that a CA follows in processing certificate requests, issuing and revoking certificates, and publishing CRLs. Usually, a CA advertises its policy in the form of certification practice statement (CPS). A CA policy can be acquired through out-of-band means such as phone, disk, and email. As different CAs might use different methods to examine the binding of a public key with an entity, make sure that you understand the CA policy before selecting a trusted CA for certificate request.

PKI architecture

A PKI system consists of entities, a CA, a registration authority (RA) and a PKI repository.

Figure 49 PKI architecture



- Entity

  An entity is an end user of PKI products or services, such as a person, an organization, a device, or a process running on a computer.
- CA

  A CA is a trusted authority responsible for issuing and managing digital certificates. A CA issues certificates, specifies the validity periods of certificates, and revokes certificates as needed by publishing CRLs.
- RA

  A registration authority (RA) is an extended part of a CA or an independent authority. An RA can implement functions including identity authentication, CRL management, key pair generation and key pair backup. The PKI standard recommends that an independent RA be used for registration management to achieve higher security.
- PKI repository

  A PKI repository can be a Lightweight Directory Access Protocol (LDAP) server or a common database. It stores and manages information like certificate requests, certificates, keys, CRLs and logs when it provides a simple query function.

  LDAP is a protocol for accessing and managing PKI information. An LDAP server stores user information and digital certificates from the RA server and provides directory navigation service. From an LDAP server, an entity can retrieve local and CA certificates of its own as well as certificates of other entities.

PKI operation

In a PKI-enabled network, an entity can request a local certificate from the CA and the device can check the validity of certificates. Here is how it operates:

1. An entity submits a certificate request to the RA.
2. The RA reviews the identity of the entity and then sends the identity information and the public key with a digital signature to the CA.
3. The CA verifies the digital signature, approves the application, and issues a certificate.
4. The RA receives the certificate from the CA, sends it to the LDAP server or other distribution point to provide directory navigation service, and notifies the entity that the certificate is successfully issued.
5. The entity retrieves the certificate. With the certificate, the entity can communicate with other entities safely through encryption and digital signature.
6. The entity makes a request to the CA when it needs to revoke its certificate. The CA approves the request, updates the CRLs and publishes the CRLs on the LDAP server or other distribution point.

PKI applications

The PKI technology can satisfy the security requirements of online transactions. As an infrastructure, PKI has a wide range of applications. Here are some application examples.

- VPN

  A virtual private network (VPN) is a private data communication network built on the public communication infrastructure. A VPN can leverage network layer security protocols (for instance, IPsec) in conjunction with PKI-based encryption and digital signature technologies for confidentiality.

- Secure email

  Emails require confidentiality, integrity, authentication, and non-repudiation. PKI can address these needs. The secure email protocol that is developing rapidly is Secure/Multipurpose Internet Mail Extensions (S/MIME), which is based on PKI and allows for transfer of encrypted mails with signature.

- Web security

  For Web security, two peers can establish an SSL connection first for transparent and secure communications at the application layer. With PKI, SSL enables encrypted communications between a browser and a server. Both of the communication parties can verify each other's identity through digital certificates.

PKI configuration task list

Task	Remarks
Configuring an entity DN	Required.
Configuring a PKI domain	Required.
Submitting a PKI certificate request • Submitting a certificate request in auto mode • Submitting a certificate request in manual mode	Required. Use either approach.
Retrieving a certificate manually	Optional.
Configuring PKI certificate verification	Optional.
Destroying a local RSA key pair	Optional.

Task	Remarks
Deleting a certificate	Optional.
Configuring an access control policy	Optional.

Configuring an entity DN

A certificate is the binding of a public key and the identity information of an entity, where the identity information is identified by an entity distinguished name (DN). A CA identifies a certificate applicant uniquely by entity DN.

An entity DN is defined by these parameters:

- Common name of the entity.
- Country code of the entity, a standard 2-character code. For example, CN represents China and US represents the United States.
- Fully qualified domain name (FQDN) of the entity, a unique identifier of an entity on the network. It consists of a host name and a domain name and can be resolved to an IP address. For example, **www.whatever.com** is an FQDN, where **www** is a host name and **whatever.com** a domain name.
- IP address of the entity.
- Locality where the entity resides.
- Organization to which the entity belongs.
- Unit of the entity in the organization.
- State where the entity resides.

The configuration of an entity DN must comply with the CA certificate issue policy. You must determine, for example, which entity DN parameters are mandatory and which are optional. Otherwise, certificate requests might be rejected.

To configure an entity DN:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an entity and enter its view.	**pki entity** *entity-name*	No entity exists by default.
3. Configure the common name for the entity.	**common-name** *name*	Optional. No common name is specified by default.
4. Configure the country code for the entity.	**country** *country-code-str*	Optional. No country code is specified by default.
5. Configure the FQDN for the entity.	**fqdn** *name-str*	Optional. No FQDN is specified by default.
6. Configure the IP address for the entity.	**ip** *ip-address*	Optional. No IP address is specified by default.

Step	Command	Remarks
7. Configure the locality for the entity.	**locality** *locality-name*	Optional. No locality is specified by default.
8. Configure the organization name for the entity.	**organization** *org-name*	Optional. No organization is specified by default.
9. Configure the unit name for the entity.	**organization-unit** *org-unit-name*	Optional. No unit is specified by default.
10. Configure the state or province for the entity.	**state** *state-name*	Optional. No state or province is specified by default.

NOTE:

The Windows 2000 CA server has some restrictions on the data length of a certificate request. If the entity DN in a certificate request goes beyond a certain limit, the server will not respond to the certificate request.

Configuring a PKI domain

Before requesting a PKI certificate, an entity needs to be configured with some enrollment information, which is referred to as a PKI domain. A PKI domain is only intended for convenient reference by applications like SSL, and only has local significance. A PKI domain configured on a switch is invisible to the CA and other switches, and each PKI domain has its own parameters.

A PKI domain defines these parameters:

- **Trusted CA**—An entity requests a certificate from a trusted CA.
- **Entity**—A certificate applicant uses an entity to provide its identity information to a CA.
- **RA**—Generally, an independent RA is in charge of certificate request management. It receives the registration request from an entity, examines its qualification, and determines whether to ask the CA to sign a digital certificate. The RA only examines the application qualification of an entity; it does not issue any certificate. Sometimes, the registration management function is provided by the CA, in which case no independent RA is required. It is a good practice to deploy an independent RA.
- **URL of the registration server**—An entity sends a certificate request to the registration server through Simple Certification Enrollment Protocol (SCEP), a dedicated protocol for an entity to communicate with a CA. This URL is also called the certificate request URL.
- **Polling interval and count**—After an applicant makes a certificate request, the CA might need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed. You can configure the polling interval and count to query the request status.
- **IP address of the LDAP server**—An LDAP server is usually deployed to store certificates and CRLs. If this is the case, you must configure the IP address of the LDAP server.
- **Fingerprint for root certificate verification**—After receiving the root certificate of the CA, an entity needs to verify the fingerprint of the root certificate, namely, the hash value of the root certificate content. This hash value is unique to every certificate. If the fingerprint of the root certificate does not match the one configured for the PKI domain, the entity will reject the root certificate.

Configuration guidelines

- Up to two PKI domains can be created on a switch.
- The CA name is required only when you retrieve a CA certificate. It is not used when in local certificate request.
- The certificate request URL does not support domain name resolution.

Configuration procedure

To configure a PKI domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a PKI domain and enter its view.	**pki domain** *domain-name*	No PKI domain exists by default.
3. Specify the trusted CA.	**ca identifier** *name*	No trusted CA is specified by default.
4. Specify the entity for certificate request.	**certificate request entity** *entity-name*	No entity is specified by default. The specified entity must exist.
5. Specify the authority for certificate request.	**certificate request from** { **ca** | **ra** }	No authority is specified by default.
6. Configure the certificate request URL.	**certificate request url** *url-string*	No certificate request URL is configured by default.
7. Configure the polling interval and attempt limit for querying the certificate request status.	**certificate request polling** { **count** *count* | **interval** *minutes* }	Optional. The polling is executed for up to 50 times at the interval of 20 minutes by default.
8. Specify the LDAP server.	**ldap-server ip** *ip-address* [**port** *port-number*] [**version** *version-number*]	Optional. No LDP server is specified by default.
9. Configure the fingerprint for root certificate verification.	**root-certificate fingerprint** { **md5** | **sha1** } *string*	Required when the certificate request mode is auto and optional when the certificate request mode is manual. In the latter case, if you do not configure this command, the fingerprint of the root certificate must be verified manually. No fingerprint is configured by default.

Submitting a PKI certificate request

When requesting a certificate, an entity introduces itself to the CA by providing its identity information and public key, which will be the major components of the certificate. A certificate request can be submitted to a CA in offline mode or online mode. In offline mode, a certificate request is submitted to a CA by an "out-of-band" means such as phone, disk, or email.

An online certificate request can be submitted in manual mode or auto mode.

Submitting a certificate request in auto mode

IMPORTANT:

In auto mode, an entity does not automatically re-request a certificate to replace a certificate that is expiring or has expired. After the certificate expires, the service using the certificate might be interrupted.

In auto mode, an entity automatically requests a certificate from the CA server through SCEP if it has no local certificate for an application working with PKI, and then retrieves the certificate and saves the certificate locally. Before requesting a certificate, if the PKI domain does not have the CA certificate yet, the entity automatically retrieves the CA certificate.

To configure an entity to submit a certificate request in auto mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter PKI domain view.	**pki domain** *domain-name*	N/A
3. Set the certificate request mode to auto.	**certificate request mode auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*] *	Manual by default

Submitting a certificate request in manual mode

In manual mode, you must submit a local certificate request for an entity. Before the request, you must retrieve a CA certificate or generate a key pair for the PKI domain if the domain do not have the CA certificate or the key pair.

The CA certificate in the PKI domain is used to verify the authenticity and validity of a local certificate.

Generating a key pair is an important step in certificate request. The key pair includes a public key and a private key. The private key is kept by the user. The public key is transferred to the CA along with some other information. For more information about RSA key pair configuration, see "Managing public keys."

Configuration guidelines

- If a PKI domain already has a local certificate, creating an RSA key pair might result in inconsistency between the key pair and the certificate. To generate a new RSA key pair, delete the local certificate and then execute the **public-key local create** command (see *Security Command Reference*).
- A newly created key pair will overwrite the existing one. If you perform the **public-key local create** command in the presence of a local RSA key pair, the system will ask you whether you want to overwrite the existing one.
- If a PKI domain already has a local certificate, you cannot request another certificate for it. This helps avoid inconsistency between the certificate and the registration information resulting from configuration changes. Before requesting a new certificate, use the **pki delete-certificate** command to delete the existing local certificate and the CA certificate stored locally.
- When it is impossible to request a certificate from the CA through SCEP, you can print the request information or save the request information to a local file, and then send the printed information or saved file to the CA by an out-of-band means. To print the request information, use the **pki**

request-certificate domain command with the **pkcs10** keyword. To save the request information to a local file, use the **pki request-certificate domain** command with the **pkcs10 filename** *filename* option.

- Make sure the clocks of the entity and the CA are synchronous. Otherwise, the validity period of the certificate will be abnormal.
- The configuration made by the **pki request-certificate domain** command is not saved in the configuration file.

Configuration procedure

To submit a certificate request in manual mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter PKI domain view.	**pki domain** *domain-name*	N/A
3. Set the certificate request mode to manual.	**certificate request mode manual**	Optional. Manual by default.
4. Return to system view.	**quit**	N/A
5. Retrieve a CA certificate manually.	See "Retrieving a certificate manually"	N/A
6. Generate a local RSA key pair.	**public-key local create rsa**	No local RSA key pair exists by default.
7. Submit a local certificate request manually.	**pki request-certificate domain** *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]	N/A

Retrieving a certificate manually

You can download CA certificates, local certificates, or peer entity certificates from the CA server and save them locally. To do so, use either the offline mode or the online mode. In offline mode, you must retrieve a certificate by an out-of-band means like FTP, disk, or email, and then import it into the local PKI system.

Certificate retrieval serves the following purposes:

- Locally store the certificates associated with the local security domain for improved query efficiency and reduced query count
- Prepare for certificate verification

Configuration guidelines

- Before retrieving a local certificate in online mode, be sure to complete the LDAP server configuration.
- If a PKI domain already has a CA certificate, you cannot retrieve another CA certificate for it. This restriction helps avoid inconsistency between the certificate and registration information resulted from configuration changes. To retrieve a new CA certificate, use the **pki delete-certificate** command to delete the existing CA certificate and the local certificate first.

- The configuration made by the **pki retrieval-certificate** configuration is not saved in the configuration file.
- Make sure the switch's system time falls in the validity period of the certificate so that the certificate is valid.

Configuration procedure

To retrieve a certificate manually:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Retrieve a certificate manually.	• In online mode: **pki retrieval-certificate** { **ca** | **local** } **domain** *domain-name* • In offline mode: **pki import-certificate** { **ca** | **local** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]	Use either command.

Configuring PKI certificate verification

A certificate needs to be verified before being used. Certificate verification can examine whether the certificate is signed by the CA and whether the certificate has expired or been revoked.

You can specify whether to perform CRL checking during certificate verification. If you enable CRL checking, CRLs will be used in verification of a certificate, and you must retrieve the CA certificate and CRLs to the local switch before the certificate verification. If you disable CRL checking, you only need to retrieve the CA certificate.

Configuration guidelines

- The CRL update period defines the interval at which the entity downloads CRLs from the CRL server. The CRL update period setting manually configured on the switch is prior to that carried in the CRLs.
- The configuration made by the **pki retrieval-crl domain** command is not saved in the configuration file.

Configuring CRL-checking-enabled PKI certificate verification

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PKI domain view.	**pki domain** *domain-name*	N/A
3.	Specify the URL of the CRL distribution point.	**crl url** *url-string*	Optional. No CRL distribution point URL is specified by default.

Step		Command	Remarks
4.	Set the CRL update period.	**crl update-period** *hours*	Optional. By default, the CRL update period depends on the next update field in the CRL file.
5.	Enable CRL checking.	**crl check enable**	Optional. Enabled by default.
6.	Return to system view.	**quit**	N/A
7.	Retrieve the CA certificate.	See "Retrieving a certificate manually"	N/A
8.	Retrieve CRLs.	**pki retrieval-crl domain** *domain-name*	N/A
9.	Verify the validity of a certificate.	**pki validate-certificate** { **ca** | **local** } **domain** *domain-name*	N/A

Configuring CRL-checking-disabled PKI certificate verification

To configure CRL-checking-disabled PKI certificate verification:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter PKI domain view.	**pki domain** *domain-name*	N/A
3.	Disable CRL checking.	**crl check disable**	Enabled by default
4.	Return to system view.	**quit**	N/A
5.	Retrieve the CA certificate.	See "Retrieving a certificate manually"	N/A
6.	Verify the validity of the certificate.	**pki validate-certificate** { **ca** | **local** } **domain** *domain-name*	N/A

Destroying a local RSA key pair

A certificate has a lifetime, which is determined by the CA. When the private key leaks or the certificate is about to expire, you can destroy the old RSA key pair and then create a pair to request a new certificate.

To destroy a local RSA key pair:

Step		Command
1.	Enter system view.	**system-view**
2.	Destroy a local RSA key pair.	**public-key local destroy rsa**

For more information about the **public-key local destroy** command, see *Security Command Reference*.

Deleting a certificate

When a certificate requested manually is about to expire or you want to request a new certificate, you can delete the current local certificate or CA certificate.

To delete a certificate:

Step	Command
1. Enter system view.	**system-view**
2. Delete certificates.	**pki delete-certificate** { **ca** | **local** } **domain** *domain-name*

Configuring an access control policy

By configuring a certificate attribute access control policy, you can further control access to the server, providing additional security for the server.

To configure a certificate attribute access control policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a certificate attribute group and enter its view.	**pki certificate attribute-group** *group-name*	No certificate attribute group exists by default.
3. Configure an attribute rule for the certificate issuer name, certificate subject name, or alternative subject name.	**attribute** *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*	Optional. No restriction exists on the issuer name, certificate subject name and alternative subject name by default.
4. Return to system view.	**quit**	N/A
5. Create a certificate attribute access control policy and enter its view.	**pki certificate access-control-policy** *policy-name*	No access control policy exists by default.
6. Configure a certificate attribute access control rule.	**rule** [*id*] { **deny** | **permit** } *group-name*	No access control rule exists by default. A certificate attribute group must exist to be associated with a rule.

Displaying and maintaining PKI

Task	Command	Remarks
Display the contents or request status of a certificate.	**display pki certificate** { { **ca** | **local** } **domain** *domain-name* | **request-status** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display CRLs.	**display pki crl domain** *domain-name* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about certificate attribute groups.	**display pki certificate attribute-group** { *group-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about certificate attribute access control policies.	**display pki certificate access-control-policy** { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

PKI configuration examples

Unless otherwise noted, devices in the configuration examples are operating in non-FIPS mode.

When the CA uses Windows Server, the SCEP add-on is required, and you must use the **certificate request from ra** command to specify that the entity request a certificate from an RA.

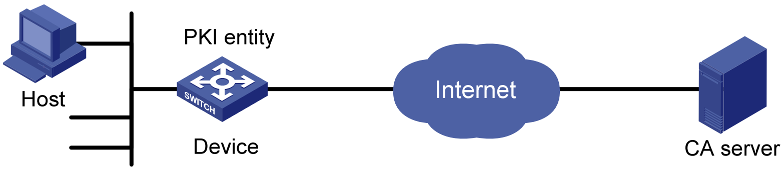
When the CA uses RSA Keon, the SCEP add-on is not required, and you must use the **certificate request from ca** command to specify that the entity request a certificate from a CA.

Certificate request from an RSA Keon CA server

Network requirements

The switch submits a local certificate request to the CA server. The switch acquires the CRLs for certificate verification.

Figure 50 Network diagram



Configuring the CA server

1. Create a CA server named **myca**:

   In this example, you need to configure these basic attributes on the CA server at first:

   - **Nickname**—Name of the trusted CA.
   - **Subject DN**—DN information of the CA, including the Common Name (CN), Organization Unit (OU), Organization (O), and Country (C).

   Use the default values for the other attributes.

2. Configure extended attributes:

   After configuring the basic attributes, perform configuration on the jurisdiction configuration page of the CA server. This includes selecting the proper extension profiles, enabling the SCEP autovetting function, and adding the IP address list for SCEP autovetting.

3. Configure the CRL distribution behavior:

   After completing the configuration, you must perform CRL related configurations. In this example, select the local CRL distribution mode of Hypertext Transfer Protocol (HTTP) and set the HTTP URL to http://4.4.4.133:447/myca.crl.

   After the configuration, make sure the system clock of the switch is synchronous to that of the CA, so that the switch can request certificates and retrieve CRLs properly.

Configuring the switch

1. Configure the entity name as **aaa** and the common name **as device**.

```
<Device> system-view
[Device] pki entity aaa
[Device-pki-entity-aaa] common-name device
[Device-pki-entity-aaa] quit
```

2. Configure the PKI domain:

   # Create PKI domain **torsa** and enter its view.

```
[Device] pki domain torsa
```

   # Configure the name of the trusted CA as **myca**.

```
[Device-pki-domain-torsa] ca identifier myca
```

   # Configure the URL of the registration server in the format of 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://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

   # Set the registration authority to **CA**.

```
[Device-pki-domain-torsa] certificate request from ca
```

   # Specify the entity for certificate request as **aaa**.

```
[Device-pki-domain-torsa] certificate request entity aaa
```

   # Configure the URL for the CRL distribution point.

```
[Device-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl
[Device-pki-domain-torsa] quit
```

3. Generate a local key pair using RSA:

```
[Device] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++
```

4. Apply for certificates:

   # Retrieve the CA certificate and save it locally.

```
[Device] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while......
The trusted CA's finger print is:
    MD5  fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB
    SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment......
CA certificates retrieval success.
```

   # Retrieve CRLs and save them locally.

```
[Device] pki retrieval-crl domain torsa
Connecting to server for retrieving CRL. Please wait a while.....
CRL retrieval success!
```

   # Request a local certificate manually.

```
[Device] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait......
[Device]
Enrolling the local certificate,please wait a while......
Certificate request Successfully!
Saving the local certificate to device......
Done!
```

Verifying the configuration

# Display information about the retrieved local certificate.

```
[Device] display pki certificate local domain torsa
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9A96A48F 9A509FD7 05FFF4DF 104AD094
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            C=cn
            O=org
            OU=test
            CN=myca
        Validity
            Not Before: Jan  8 09:26:53 2012 GMT
            Not After : Jan  8 09:26:53 2012 GMT
        Subject:
            CN=device
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00D67D50 41046F6A 43610335 CA6C4B11
                    F8F89138 E4E905BD 43953BA2 623A54C0
                    EA3CB6E0 B04649CE C9CDDD38 34015970
                    981E96D9 FF4F7B73 A5155649 E583AC61
                    D3A5C849 CBDE350D 2A1926B7 0AE5EF5E
                    D1D8B08A DBF16205 7C2A4011 05F11094
                    73EB0549 A65D9E74 0F2953F2 D4F0042F
                    19103439 3D4F9359 88FB59F3 8D4B2F6C
                    2B
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 CRL Distribution Points:
            URI:http://4.4.4.133:447/myca.crl

    Signature Algorithm: sha1WithRSAEncryption
        836213A4 F2F74C1A 50F4100D B764D6CE
        B30C0133 C4363F2F 73454D51 E9F95962
        EDE9E590 E7458FA6 765A0D3F C4047BC2
        9C391FF0 7383C4DF 9A0CCFA9 231428AF
        987B029C C857AD96 E4C92441 9382E798
        8FCC1E4A 3E598D81 96476875 E2F86C33
        75B51661 B6556C5E 8F546E97 5197734B
        C8C29AC7 E427C8E4 B9AAF5AA 80A75B3C
```

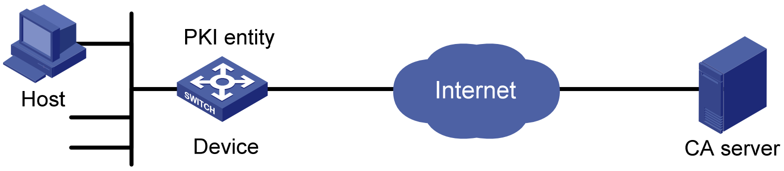
You can also use **display pki certificate ca domain** and **display pki crl domain** to display detailed information about the CA certificate and CRLs. For more information about the commands, see *Security Command Reference*.

Certificate request from a Windows 2003 CA server

Network requirements

Configure PKI entity Device to request a local certificate from the CA server.

Figure 51 Network diagram



Configuring the CA server

1. Install the certificate service suites:
   a. Select **Control Panel** > **Add or Remove Programs** from the start menu.
   b. Select **Add/Remove Windows Components** > **Certificate Services**.
   c. Click **Next** to begin the installation.
2. Install the SCEP add-on:

   Because a CA server running the Windows 2003 server does not support SCEP by default, you must install the SCEP add-on so that the switch can register and obtain its certificate automatically.

After the SCEP add-on installation completes, a URL is displayed, which you must configure on the switch as the URL of the server for certificate registration.

3. Modify the certificate service attributes:
   a. Select **Control Panel** > **Administrative Tools** > **Certificate Authority** from the start menu.

      If the CA server 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 select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**.
4. Modify the Internet Information Services (IIS) attributes:
   a. Select **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager** from the start menu.
   b. Select **Web Sites** from the navigation tree.
   c. Right-click **Default Web Site** and select **Properties** > **Home Directory**.
   d. Specify the path for certificate service in the **Local path** text box.

      To avoid conflict with existing services, specify an available port number as the TCP port number of the default website.

After completing the configuration, make sure the system clock of the switch is synchronous to that of the CA server, so that that the switch can request a certificate normally.

Configuring the switch

1. Configure the entity name as **aaa** and the common name **as device**.

```
<Device> system-view
[Device] pki entity aaa
[Device-pki-entity-aaa] common-name device
[Device-pki-entity-aaa] quit
```

2. Configure the PKI domain:

   # Create PKI domain **torsa** and enter its view.

```
[Device] pki domain torsa
```

   # Configure the name of the trusted CA as **myca**.

```
[Device-pki-domain-torsa] ca identifier myca
```

   # Configure the URL of the registration server in the format of http://host:port/certsrv/mscep/mscep.dll, where host:port indicates the IP address and port number of the CA server.

```
[Device-pki-domain-torsa] certificate request url
http://4.4.4.1:8080/certsrv/mscep/mscep.dll
```

   # Set the registration authority to **RA**.

```
[Device-pki-domain-torsa] certificate request from ra
```

   # Specify the entity for certificate request as **aaa**.

```
[Device-pki-domain-torsa] certificate request entity aaa
```

3. Generate a local key pair using RSA:

```
[Device] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
```

```
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++
```

4. Apply for certificates:

   # Retrieve the CA certificate and save it locally.

```
[Device] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while......
The trusted CA's finger print 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 finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment......
CA certificates retrieval success.
```

   # Request a local certificate manually.

```
[Device] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait......
[Device]
Enrolling the local certificate,please wait a while......
Certificate request Successfully!
Saving the local certificate to device......
Done!
```

Verifying the configuration

# Display information about the retrieved local certificate.

```
[Device] display pki certificate local domain torsa
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48FA0FD9 00000000 000C
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            CN=myca
        Validity
            Not Before: Feb 21 12:32:16 2012 GMT
            Not After : Feb 21 12:42:16 2012 GMT
        Subject:
            CN=device
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
```

```
                Modulus (1024 bit):
                    00A6637A 8CDEA1AC B2E04A59 F7F6A9FE
                    5AEE52AE 14A392E4 E0E5D458 0D341113
                    0BF91E57 FA8C67AC 6CE8FEBB 5570178B
                    10242FDD D3947F5E 2DA70BD9 1FAF07E5
                    1D167CE1 FC20394F 476F5C08 C5067DF9
                    CB4D05E6 55DC11B6 9F4C014D EA600306
                    81D403CF 2D93BC5A 8AF3224D 1125E439
                    78ECEFE1 7FA9AE7B 877B50B8 3280509F
                    6B
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
            B68E4107 91D7C44C 7ABCE3BA 9BF385F8 A448F4E1
            X509v3 Authority Key Identifier:
            keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

            X509v3 CRL Distribution Points:
            URI:http://l00192b/CertEnroll/CA%20server.crl
            URI:file://\\l00192b\CertEnroll\CA server.crl

            Authority Information Access:
            CA Issuers - URI:http://l00192b/CertEnroll/l00192b_CA%20server.crt
            CA Issuers - URI:file://\\l00192b\CertEnroll\l00192b_CA server.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
        81029589 7BFA1CBD 20023136 B068840B
(Omitted)
```

You can also use some other **display** commands to display more information about the CA certificate. For more information about the **display pki certificate ca domain** command, see *Security Command Reference*.

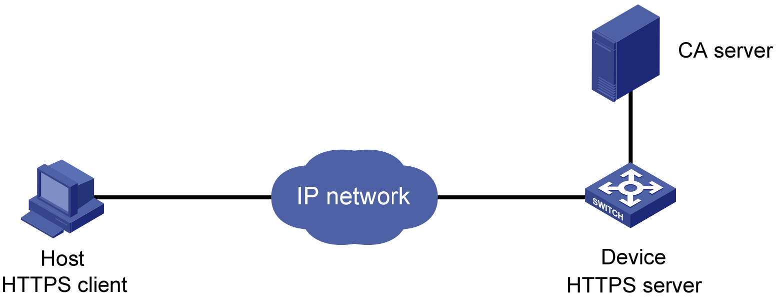
Certificate attribute access control policy configuration example

Network requirements

The client accesses the remote HTTP Secure (HTTPS) server through the HTTPS protocol.

Configure SSL to make sure that only legal clients log into the HTTPS server, and create a certificate attribute access control policy to control access to the HTTPS server.

Figure 52 Network diagram



Configuration procedure

The configuration procedure involves SSL configuration and HTTPS configuration. For more information about SSL configuration, see "Configuring SSL." For more information about HTTPS configuration, see *Fundamentals Configuration Guide*.

The PKI domain to be referenced by the SSL policy must exist. For how to configure a PKI domain, see "Configure the PKI domain:."

The configuration procedure is as follows:

1. Configure the HTTPS server:

   # Configure the SSL policy for the HTTPS server to use.

   ```
   <Device> system-view
   [Device] ssl server-policy myssl
   [Device-ssl-server-policy-myssl] pki-domain 1
   [Device-ssl-server-policy-myssl] client-verify enable
   [Device-ssl-server-policy-myssl] quit
   ```

2. Configure the certificate attribute group:

   # Create certificate attribute group **mygroup1** and add two attribute rules. The first rule defines that the DN of the subject name includes the string **aabbcc**, and the second rule defines that the IP address of the certificate issuer is 10.0.0.1.

   ```
   [Device] pki certificate attribute-group mygroup1
   [Device-pki-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn aabbcc
   [Device-pki-cert-attribute-group-mygroup1] attribute 2 issuer-name ip equ 10.0.0.1
   [Device-pki-cert-attribute-group-mygroup1] quit
   ```

   # Create certificate attribute group **mygroup2** and add two attribute rules. The first rule defines that the FQDN of the alternative subject name does not include the string of **apple**, and the second rule defines that the DN of the certificate issuer name includes the string **aabbcc**.

   ```
   [Device] pki certificate attribute-group mygroup2
   [Device-pki-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn
   apple
   [Device-pki-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn aabbcc
   [Device-pki-cert-attribute-group-mygroup2] quit
   ```

3. Create a certificate attribute access control policy named **myacp** and add two access control rules.

   ```
   [Device] pki certificate access-control-policy myacp
   [Device-pki-cert-acp-myacp] rule 1 deny mygroup1
   [Device-pki-cert-acp-myacp] rule 2 permit mygroup2
   [Device-pki-cert-acp-myacp] quit
   ```

4. Apply the SSL server policy and certificate attribute access control policy to HTTPS service and enable HTTPS service:

   # Apply SSL server policy **myssl** to HTTPS service.

   ```
   [Device] ip https ssl-server-policy myssl
   ```

   # Apply the certificate attribute access control policy of **myacp** to HTTPS service.

   ```
   [Device] ip https certificate access-control-policy myacp
   ```

   # Enable HTTPS service.

   ```
   [Device] ip https enable
   ```

Troubleshooting PKI

Failed to retrieve a CA certificate

Symptom

Failed to retrieve a CA certificate.

Analysis

- The network connection is not proper. For example, the network cable might be damaged or loose.
- No trusted CA is specified.
- The URL of the registration server for certificate request is not correct or not configured.
- No authority is specified for certificate request.
- The system clock of the switch is not synchronized with that of the CA.

Solution

- Make sure the network connection is physically proper.
- Check that the required commands are configured properly.
- Use the **ping** command to verify that the RA server is reachable.
- Specify the authority for certificate request.
- Synchronize the system clock of the switch with that of the CA.

Failed to request a local certificate

Symptom

Failed to request a local certificate.

Analysis

- The network connection is not proper. For example, the network cable might be damaged or loose.
- No CA certificate has been retrieved.
- The current key pair has been bound to a certificate.
- No trusted CA is specified.
- The URL of the registration server for certificate request is not correct or not configured.
- No authority is specified for certificate request.
- Some required parameters of the entity DN are not configured.

Solution

- Make sure the network connection is physically proper.
- Retrieve a CA certificate.
- Regenerate a key pair.
- Specify a trusted CA.
- Use the **ping** command to verify that the RA server is reachable.
- Specify the authority for certificate request.
- Configure the required entity DN parameters.

Failed to retrieve CRLs

Symptom

Failed to retrieve CRLs.

Analysis

- The network connection is not proper. For example, the network cable might be damaged or loose.
- No CA certificate has been retrieved before you try to retrieve CRLs.
- The IP address of LDAP server is not configured.
- The CRL distribution URL is not configured.
- The LDAP server version is wrong.
- The domain name of the CRL distribution point failed to be resolved.

Solution

- Make sure the network connection is physically proper.
- Retrieve a CA certificate.
- Specify the IP address of the LDAP server.
- Specify the CRL distribution URL.
- Re-configure the LDAP version.
- Configure the correct DNS server that can resolve the domain name of the CRL distribution point.

Configuring IPsec

The term "router" in this document refers to both routers and switches.

A switch in IRF mode does not support IPsec automatic negotiation.

IPsec configuration is available only for the switches in FIPS mode. For more information about FIPS mode, see "Configuring FIPS."

Overview

IP Security (IPsec) is a security framework defined by the Internet Engineering Task Force (IETF) for securing IP communications.

IPsec provides the following security services at the IP layer for two communication parties:

- 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 these benefits:

- Reduced key negotiation overheads and simplified maintenance by supporting the Internet Key Exchange (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.

IPsec comprises a set of protocols, including Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE), and algorithms for authentication and encryption. AH and ESP provides security services and IKE performs automatic key exchange.

Basic concepts

Security protocols

IPsec comes with two security protocols:

- AH (protocol 51)—Provides data origin authentication, data integrity, and anti-replay services by adding an AH header to each IP packet. AH is suitable only for transmitting non-critical data because it cannot prevent eavesdropping, although it can prevent data tampering. AH supports authentication algorithms such as Message Digest (MD5) and Secure Hash Algorithm (SHA-1).
- ESP (protocol 50)—Provides data encryption as well as data origin authentication, data integrity, and anti-replay services by inserting an ESP header and an ESP trailer in IP packets. Unlike AH, ESP encrypts data before encapsulating the data to guarantee data confidentiality. ESP supports encryption algorithms such as Data Encryption Standard (DES), 3DES, and Advanced Encryption

Standard (AES), and authentication algorithms such as MD5 and SHA-1. The authentication function is optional to ESP.

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. Figure 53 shows the format of IPsec packets.

Security association

A security association (SA) is an agreement negotiated between two communicating parties called IPsec peers. It comprises a set of parameters for data protection, including security protocols, encapsulation mode, authentication and encryption algorithms, and shared keys and their lifetime. SAs can be set up manually or through IKE.

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.

An SA is uniquely identified by a triplet, which consists of the security parameter index (SPI), destination IP address, and security protocol identifier (AH or ESP).

An SPI is a 32-bit number for uniquely identifying an SA. It is transmitted in the AH/ESP header. A manually configured SA requires an SPI to be specified manually for it; an IKE created SA will have an SPI generated at random.

A manually configured SA never ages out. An IKE created SA has a specified period of lifetime, which comes in two types:

- Time-based lifetime, which defines how long the SA can be valid after it is created.
- Traffic-based lifetime, which defines the maximum traffic that the SA can process.

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.

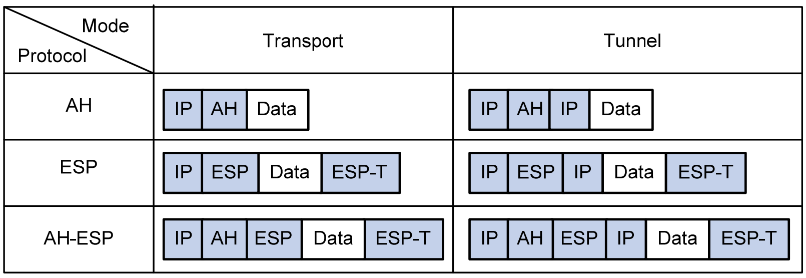
Encapsulation modes

IPsec supports the following IP packet encapsulation modes:

- Tunnel mode—IPsec protects the entire IP packet, including both the IP header and the payload. It uses the entire IP packet to calculate an AH or ESP header, and then encapsulates the original IP packet and the AH or ESP header with a new IP header. If you use ESP, an ESP trailer is also encapsulated. Tunnel mode is typically used for protecting gateway-to-gateway communications.
- Transport mode—IPsec protects only the IP payload. It uses only the IP payload to calculate the AH or ESP header, and inserts the calculated header between the original IP header and payload. If you use ESP, an ESP trailer is also encapsulated. The transport mode is typically used for protecting host-to-host or host-to-gateway communications.

Figure 53 shows how the security protocols encapsulate an IP packet in different encapsulation modes. Data represents the transport layer data.

Figure 53 Encapsulation by security protocols in different modes



Mode / Protocol	Transport	Tunnel
AH	IP | AH | Data	IP | AH | IP | Data
ESP	IP | ESP | Data | ESP-T	IP | ESP | IP | Data | ESP-T
AH-ESP	IP | AH | ESP | Data | ESP-T	IP | AH | ESP | IP | Data | ESP-T

Authentication algorithms and encryption algorithms

1. 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. If the resulting digests are identical, the packet is considered intact.

IPsec supports the following hash algorithms for authentication:

- MD5, which takes a message of arbitrary length as input and produces a 128-bit message digest.
- SHA-1, which takes a message of a maximum length less than the 64th power of 2 in bits as input and produces a 160-bit message digest.

Compared with SHA-1, MD5 is faster but less secure.

2. Encryption algorithms

IPsec mainly 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:

- Data Encryption Standard (DES), which encrypts a 64-bit plain text block with a 56-bit key. DES is the least secure but the fastest algorithm. It is sufficient for general security requirements.
- Triple DES (3DES), which encrypts plain text 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.
- Advanced Encryption Standard (AES), which encrypts plain text data with a 128-bit, 192-bit, or 256-bit key. AES provides the highest security strength and is slower than 3DES.

IPsec SA setup modes

There are two IPsec SA setup modes:

- Manual mode. In this mode, you manually configure and maintain all SA settings. Advanced features like periodical key update are not available. However, this mode implements IPsec independently of IKE.
- ISAKMP mode. In this mode, IKE automatically negotiates and maintains IPsec SAs for IPsec.

If the number of IPsec tunnels in your network is small, use the manual mode. If the number of IPsec tunnels is large, use the ISAKMP mode.

IPsec tunnel

An IPsec tunnel is a bidirectional channel created between two peers. An IPsec tunnel comprises one or more pairs of SAs.

Protocols and standards

Protocols and standards relevant to IPsec are as follows:

- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2402, *IP Authentication Header*
- RFC 2406, *IP Encapsulating Security Payload*

Configuring IPsec

IPsec can be implemented based on only ACLs. ACL-based IPsec uses ACLs to identify the data flows to be protected. To implement ACL-based IPsec, configure IPsec policies, reference ACLs in the policies, and apply the policies to physical interfaces. By using ACLs, you can customize IPsec policies as needed, implementing IPsec flexibly.

Implementing ACL-based IPsec

To ensure a successful ACL-based IPsec setup, read the feature restrictions and guidelines carefully before you configure an ACP-based IPsec tunnel.

Feature restrictions and guidelines

ACL-based IPsec can protect only traffic that is generated by the device and traffic that is destined for the device. You cannot use an ACL-based IPsec tunnel to protect user traffic. In the ACL that is used to identify IPsec protected traffic, ACL rules that match traffic forwarded through the device do not take effect. For example, an ACL-based IPsec tunnel can protect log messages the device sends to a log server, but it cannot protect traffic that is forwarded by the device for two hosts, even if the host-to-host traffic matches an ACL permit rule. For more information about configuring an ACL for IPsec, see "Configuring ACLs."

Typically, IKE uses UDP port 500 for communication, and AH and ESP use the protocol numbers 51 and 50, respectively. Make sure flows of these protocols are not denied on the interfaces with IKE or IPsec configured.

ACL-based IPsec configuration task list

The following is the generic configuration procedure for implementing ACL-based IPsec:

1. Configure ACLs for identifying data flows to be protected.
2. Configure IPsec proposals to specify the security protocols, authentication and encryption algorithms, and encapsulation mode.
3. Configure IPsec policies to associate data flows with IPsec proposals and 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.
4. Apply the IPsec policies to interfaces to finish IPsec configuration.

To configure ACL-based IPsec:

Task	Remarks
Configuring ACLs	Required. Basic IPsec configuration.
Configuring an IPsec proposal	

Task	Remarks
Configuring an IPsec policy	
Applying an IPsec policy group to an interface	
Configuring the IPsec session idle timeout	Optional.
Enabling ACL checking of de-encapsulated IPsec packets	Optional.
Configuring the IPsec anti-replay function	Optional.
Configuring packet information pre-extraction	Optional.

Configuring ACLs

ACLs can be used to identify traffic. They are widely used in scenarios where traffic identification is desired, such as QoS and IPsec.

Keywords in ACL rules

IPsec uses ACLs to identify data flows. 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 referenced 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. For the outbound traffic, IPsec uses the source and destination IP addresses specified in the rule to match the source and destination IP addresses of the traffic. For the returned inbound traffic, IPsec uses the destination IP address and the source IP address specified in the rule to match the source IP address and the destination IP address of the 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 function 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 and matched against the rule again. Only those that match a permit statement are processed by IPsec.

When you configure an ACL 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 and 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 the inbound traffic that does not need IPsec protection to be all dropped.
- Avoid statement conflicts in the scope of IPsec policy groups. When creating a deny statement, be careful with its matching scope and matching order relative to permit statements. The policies in an IPsec policy group 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 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. 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.

- An ACL can be specified for only one IPsec policy. ACLs referenced by IPsec policies cannot be used by other services.
- You must create a mirror image ACL rule at the remote end for each ACL rule created at the local end. Otherwise, IPsec may protect traffic in only one direction.

Mirror image ACLs

To make sure that SAs can be set up and the traffic protected by IPsec can be processed correctly at the remote peer, on the remote peer, create a mirror image ACL rule for each ACL rule created at the local peer.

If the ACL rules on peers do not form mirror images of each other, SAs can be set up only when both of the following requirements are met:

- The range specified by an ACL rule on one peer is covered by its counterpart ACL rule on the other peer.
- The peer with the narrower rule initiates SA negotiation. If a wider ACL rule is used by the SA initiator, the negotiation request may be rejected because the matching traffic is beyond the scope of the responder.

Protection modes

The switch supports IPsec for data flows in standard mode. In standard mode, one tunnel protects one data flow. The data flow permitted by an ACL rule is protected by one tunnel that is established solely for it.

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

NOTE:

To use IPsec in combination with QoS, make sure IPsec's ACL classification rules match the QoS classification rules. If the rules do not match, QoS may classify the packets of one IPsec SA to different queues, causing packets to be sent out of order. When the anti-replay function is enabled, IPsec will discard the packets beyond the anti-replay window in the inbound direction, resulting in packet loss. For more information about QoS classification rules, see *ACL and QoS Configuration Guide*.

Configuring an IPsec proposal

An IPsec proposal, part of an IPsec policy or an IPsec profile, defines the security parameters for IPsec SA negotiation, including the security protocol, the encryption and authentication algorithms, and the encapsulation mode.

To configure an IPsec proposal:

Step	Command	Remarks
1. Enter system view	**system-view**	N/A
2. Create an IPsec proposal and enter its view	**ipsec proposal** *proposal-name*	By default, no IPsec proposal exists.
3. Specify the security protocol for the proposal	**transform** { **ah** | **ah-esp** | **esp** }	Optional. ESP by default.

Step	Command	Remarks
4. Specify the security algorithms	- Specify the encryption algorithm for ESP: **esp encryption-algorithm aes** [*key-length*] - Specify the authentication algorithm for ESP: **esp authentication-algorithm sha1** - Specify the authentication algorithm for AH: **ah authentication-algorithm sha1**	Optional. For ESP, the default encryption algorithm is AES-128. For ESP and AH, the default authentication algorithm is SHA1.
5. Specify the IP packet encapsulation mode for the IPsec proposal	**encapsulation-mode** { **transport** | **tunnel** }	Optional. Tunnel mode by default. Transport mode applies only when the source and destination IP addresses of data flows match those of the IPsec tunnel.

NOTE:

- Changes to an IPsec proposal 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 using the updated parameters.
- Only when a security protocol is selected, can you configure security algorithms for it. For example, you can specify the ESP-specific security algorithms only when you select ESP as the security protocol.
- You must use both ESP encryption and authentication.

Configuring an IPsec policy

IPsec policies define which IPsec proposals should be used to protect which data flows. An IPsec policy is uniquely identified by its name and sequence number.

IPsec policies fall into two categories:

- 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.
- IPsec policy that uses IKE—The parameters are automatically negotiated through IKE.

Configuring a manual IPsec policy

To guarantee successful SA negotiations, follow these guidelines when configuring manual IPsec policies at the two ends of an IPsec tunnel:

- The IPsec policies at the two ends must have IPsec proposals that use the same security protocols, security algorithms, and encapsulation mode.
- The remote IP address configured on the local end must be the same as the IP address of the remote end.
- At each end, configure parameters for both the inbound SA and the outbound SA, and make sure that different SAs use different SPIs. SPIs for the SAs in the same direction must be different.
- 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.

Before you configure a manual IPsec policy, configure ACLs used for identifying protected traffic and IPsec transform sets.

To configure a manual IPsec policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a manual IPsec policy and enter its view.	**ipsec policy** *policy-name* *seq-number* **manual**	By default, no IPsec policy exists.
3. Assign an ACL to the IPsec policy.	**security acl** *acl-number*	By default, an IPsec policy references no ACL. An IPsec policy can reference only one ACL. If you specify multiple ACLs for an IPsec policy, only the last specified ACL takes effect.
4. Assign an IPsec proposal to the IPsec policy.	**proposal** *proposal-name*	By default, an IPsec policy references no IPsec proposal. A manual IPsec policy can reference only one IPsec proposal. To change an IPsec proposal for an IPsec policy, you must remove the current reference first.
5. Configure the two ends of the IPsec tunnel.	• Configure the local address of the tunnel: **tunnel local** *ip-address* • Configure the remote address of the tunnel: **tunnel remote** *ip-address*	Configuring the remote address of the tunnel is required. Both the local and remote addresses are not configured by default.
6. Configure an SPI for an SA.	**sa spi** { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*	By default, no SPI is configured for an SA.
7. Configure keys for the SA.	• Configure an authentication key in hexadecimal for AH: **sa authentication-hex** { **inbound** | **outbound** } **ah** [**cipher** *string-key* | **simple** *hex-key*] • Configure an authentication key in hexadecimal for ESP: **sa authentication-hex**.{ **inbound** | **outbound** } **esp** [**cipher** *string-key* | **simple** *hex-key*] • Configure an encryption key in hexadecimal for ESP: **sa encryption-hex**.{ **inbound** | **outbound** } **esp** [**cipher** *string-key* | **simple** *hex-key*]	Configure keys properly for the security protocol (AH or ESP) you have specified.

NOTE:

You cannot change the creation mode of an IPsec policy from manual to through IKE, or vice versa. To create an IPsec policy that uses IKE, delete the manual IPsec policy, and then use IKE to configure an IPsec policy.

Configuring an IPsec policy that uses IKE

To configure an IPsec policy that uses IKE, directly configure it by configuring the parameters in IPsec policy view.

Before you configure an IPsec policy that uses IKE, configure the ACLs and the IKE peer for the IPsec policy.

The parameters for the local and remote ends must match.

When you configure an IPsec policy that uses IKE, follow these guidelines:

- An IPsec policy can reference only one ACL. If you apply multiple ACLs to an IPsec policy, only the last one takes effect.
- With SAs to be established through IKE negotiation, an IPsec policy can reference up to six IPsec proposals. During negotiation, IKE searches for a fully matched IPsec proposal at the two ends of the expected IPsec tunnel. If no match is found, no SA can be set up and the packets expecting to be protected will be dropped.
- During IKE negotiation for an IPsec policy with PFS enabled, an additional key exchange is performed. If the local end uses PFS, the remote end must also use PFS for negotiation and both ends must use the same Diffie-Hellman (DH) group; otherwise, the negotiation will fail.
- An SA uses the global lifetime settings when it is not configured with lifetime settings in IPsec policy view. When negotiating to set up SAs, IKE uses the local lifetime settings or those proposed by the peer, whichever are smaller.
- You cannot change the creation mode of an IPsec policy directly. To create an IPsec policy in another creation mode, delete the current one and then configure a new IPsec policy.

To directly configure an IPsec policy that uses IKE:

Step	Command	Remark
1. Enter system view.	**system-view**	N/A
2. Create an IPsec policy that uses IKE and enter its view.	**ipsec policy** *policy-name seq-number* **isakmp**	By default, no IPsec policy exists.
3. Configure an IPsec connection name.	**connection-name** *name*	Optional. By default, no IPsec connection name is configured.
4. Assign an ACL to the IPsec policy.	**security acl** *acl-number*	By default, an IPsec policy references no ACL. An IPsec policy can reference only one ACL. If you specify multiple ACLs for an IPsec policy, only the last specified ACL takes effect.
5. Assign IPsec proposals to the IPsec policy.	**proposal** *proposal-name*&<1-6>	By default, an IPsec policy references no IPsec proposal.

Step	Command	Remark
6. Specify an IKE peer for the IPsec policy.	**ike-peer** *peer-name*	An IPsec policy cannot reference any IKE peer that is already referenced by an IPsec profile, and vice versa.
7. Enable and configure the perfect forward secrecy feature for the IPsec policy.	**pfs** { **dh-group2** | **dh-group5** | **dh-group14** }	Optional. By default, the PFS feature is not used for negotiation. For more information about PFS, see the chapter "IKE configuration."
8. Set the SA lifetime.	**sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	Optional. By default, the global SA lifetime is used.
9. Enable the IPsec policy.	**policy enable**	Optional. Enabled by default.
10. Return to system view.	**quit**	N/A
11. Set the global SA lifetime.	**ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }	Optional. 3600 seconds for time-based SA lifetime by default. 1843200 kilobytes for traffic-based SA lifetime by default.

With SAs to be established through IKE negotiation, an IPsec policy can reference up to six IPsec transform sets. During negotiation, IKE searches for a fully matched IPsec transform set at the two ends of the expected IPsec tunnel. If no match is found, no SA can be set up and the packets expecting to be protected will be dropped.

During IKE negotiation for an IPsec policy with PFS enabled, an additional key exchange is performed. If the local end uses PFS, the remote end must also use PFS for negotiation and both ends must use the same DH group. Otherwise, the negotiation will fail.

An SA uses the global lifetime settings when it is not configured with lifetime settings in IPsec policy view. When negotiating to set up SAs, IKE uses the local lifetime settings or those proposed by the peer, whichever are smaller.

You cannot change the creation mode of an IPsec policy from IKE to manual, or vice versa. To create a manual IPsec policy, delete the IKE-mode IPsec policy, and then configure the manual IPsec policy.

Applying an IPsec policy group to an interface

An IPsec policy group is a collection of IPsec policies with the same name but different sequence numbers. In an IPsec policy group, an IPsec policy with a smaller sequence number has a higher priority.

You can apply an IPsec policy group to a logical or physical interface to protect certain data flows. To cancel the IPsec protection, remove the application of the IPsec policy group.

For each packet to be sent out an IPsec protected interface, the system looks through the IPsec policies in the IPsec policy group in ascending order of sequence numbers. If an IPsec policy matches the packet, the system uses the IPsec policy to protect the packet. If no match is found, the system sends the packet out without IPsec protection.

To apply an IPsec policy group to an interface:

Step	Command
1. Enter system view.	**system-view**
2. Enter interface view.	**interface** *interface-type interface-number*
3. Apply an IPsec policy group to the interface.	**ipsec policy** *policy-name*

NOTE:

- IPsec policies can be applied only to VLAN interfaces on the switch.
- An interface can reference only one IPsec policy group. An IPsec policy can be applied to only one interface.

Configuring the IPsec session idle timeout

An IPsec session is created when the first packet matching an IPsec policy arrives. Also created is an IPsec session entry, which records the quintuplet (source IP address, destination IP address, protocol number, source port, and destination port) and the matched IPsec tunnel.

An IPsec session is automatically deleted after the idle timeout expires.

Subsequent data flows search the session entries according to the quintuplet to find a matched item. If found, the data flows are processed according to the tunnel information; otherwise, they are processed according to the original IPsec process: search the policy group or policy at the interface, and then the matched tunnel.

The session processing mechanism of IPsec saves intermediate matching procedures, improving the IPsec forwarding efficiency.

To set the IPsec session idle timeout:

Step	Command	Remark
1. Enter system view.	**system-view**	N/A
2. Set the IPsec session idle timeout.	**ipsec session idle-time** *seconds*	Optional. 300 seconds by default.

Enabling ACL checking of de-encapsulated IPsec packets

In tunnel mode, the IP packet that was encapsulated in an inbound IPsec packet may not be an object that is specified by an ACL to be protected. For example, a forged packet is not an object to be protected. If you enable ACL checking of de-encapsulated IPsec packets, all packets failing the checking will be discarded, improving the network security.

To enable ACL checking of de-encapsulated IPsec packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable ACL checking of de-encapsulated IPsec packets.	**ipsec decrypt check**	Optional. Enabled by default.

Configuring the IPsec anti-replay function

The IPsec anti-replay function protects networks against anti-replay attacks by using a sliding window mechanism called anti-replay window. This function 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 not only makes no sense, but also consumes large amounts of resources and degrades performance, resulting in DoS. IPsec anti-replay checking, when enabled, is performed before the de-encapsulation process, reducing resource waste.

In some cases, however, the sequence numbers of some normal service data packets may be out of the current sequence number range, and the IPsec anti-replay function may drop them as well, affecting the normal communications. If this happens, disable IPsec anti-replay checking or adjust the size of the anti-replay window as required.

To configure IPsec anti-replay checking:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable IPsec anti-replay checking.	**ipsec anti-replay check**	Optional. Enabled by default.
3. Set the size of the IPsec anti-replay window.	**ipsec anti-replay window** *width*	Optional. 32 by default.

△ CAUTION:

- IPsec anti-replay checking is enabled by default. Do not disable it unless it needs to be disabled.
- A wider anti-replay window results in higher resource cost and more system performance degradation, which is against the original intention of the IPsec anti-replay function. Specify an anti-replay window size that is as small as possible.

NOTE:

IPsec anti-replay checking does not affect manually created IPsec SAs. According to the IPsec protocol, only IPsec SAs negotiated by IKE support anti-replay checking.

Configuring packet information pre-extraction

If you apply both an IPsec policy and QoS policy to an interface, by default, the interface first uses IPsec and then QoS to process IP packets, and QoS classifies packets by the headers of IPsec-encapsulated packets. If you want QoS to classify packets by the headers of the original IP packets, enable the packet information pre-extraction feature.

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

To configure packet information pre-extraction:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step		Command	Remarks
2.	Enter IPsec policy view.	**ipsec policy** *policy-name* *seq-number* [**isakmp** | **manual**]	Configure either command.
3.	Enable packet information pre-extraction.	**qos pre-classify**	Disabled by default.

Displaying and maintaining IPsec

To do…	Use the command…	Remarks
Display IPsec policy information	**display ipsec policy** [**brief** | **name** *policy-name* [*seq-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPsec proposal information	**display ipsec proposal** [*proposal-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPsec SA information	**display ipsec sa** [**brief** | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPsec session information	**display ipsec session** [**tunnel-id** *integer*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPsec packet statistics	**display ipsec statistics** [**tunnel-id** *integer*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IPsec tunnel information	**display ipsec tunnel** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Clear SAs	**reset ipsec sa** [**parameters** *dest-address protocol spi* | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*]	Available in user view.
Clear IPsec sessions	**reset ipsec session** [**tunnel-id** *integer*]	Available in user view.
Clear IPsec statistics	**reset ipsec statistics**	Available in user view.

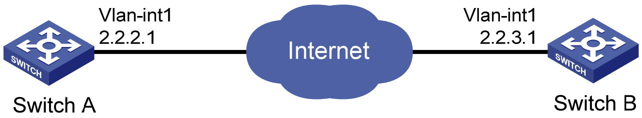
IPsec configuration examples

IKE-based IPsec tunnel for IPv4 packets configuration example

Network requirements

As shown in Figure 54, configure an IPsec tunnel between Switch A and Switch B to protect data flows between Switch A and Switch B. Configure the tunnel to use the security protocol ESP, the encryption algorithm AES-128, and the authentication algorithm HMAC-SHA1-96.

Figure 54 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 2.2.2.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

# Define an ACL to identify data flows from Switch A to 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 proposal named **tran1**.

```
[SwitchA] ipsec proposal tran1
```

# Specify the encapsulation mode as **tunnel**.

```
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

# Specify the security protocol as **ESP**.

```
[SwitchA-ipsec-proposal-tran1] transform esp
```

# Specify the algorithms for the proposal.

```
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
```

# Configure the IKE peer.

```
[SwitchA] ike peer peer
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchA-ike-peer-peer] remote-address 2.2.3.1
[SwitchA-ike-peer-peer] quit
```

# Create an IPsec policy that uses IKE for IPsec SA negotiation.

```
[SwitchA] ipsec policy map1 10 isakmp
```

# Apply the IPsec proposal.

```
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
```

# Apply the ACL.

```
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
```

# Apply the IKE peer.

```
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
```

# Apply the IPsec policy group to VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1
```

2. Configure Switch B:

# Assign an IP address to 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
```

# Define an ACL to identify data flows from Switch B to 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 proposal named **tran1**.

```
[SwitchB] ipsec proposal tran1
```

# Specify the encapsulation mode as **tunnel**.

```
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
```

# Specify the security protocol as **ESP**.

```
[SwitchB-ipsec-proposal-tran1] transform esp
```

# Specify the algorithms for the proposal.

```
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
```

# Configure the IKE peer.

```
[SwitchB] ike peer peer
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
[SwitchB-ike-peer-peer] remote-address 2.2.2.1
[SwitchB-ike-peer-peer] quit
```

# Create an IPsec policy that uses IKE for IPsec SA negotiation.

```
[SwitchB] ipsec policy use1 10 isakmp
```

# Apply the ACL.

```
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
```

# Apply the IPsec proposal.

```
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
```

# Apply the IKE peer.

```
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
[SwitchB-ipsec-policy-isakmp-use1-10] quit
```

# Apply the IPsec policy group to VLAN-interface 1.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ipsec policy use1
```

3. Verifying the configuration

After the previous configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. If IKE negotiation is successful and SAs are set up, the traffic between the two switches will be IPsec protected.

Configuring IKE

This feature is applicable only to the switches in FIPS mode. For more information about FIPS mode, see "Configuring FIPS."

Overview

Built on a framework defined by the Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange (IKE) provides automatic key negotiation and SA establishment services for IPsec, simplifying the application, management, configuration and maintenance of IPsec dramatically.

Instead of transmitting keys directly across a network, IKE peers transmit keying materials between them, and calculate shared keys respectively. Even if a third party captures all exchanged data for calculating the keys, it cannot calculate the keys.

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.

Data authentication

Data authentication involves two concepts:

- Identity authentication—Mutual identity authentication between peers. Two authentication methods are available: pre-shared key authentication and PKI-based digital signature authentication (RSA signature).
- Identity protection—Encrypts the identity information with the generated keys before sending the information.

DH

The Diffie-Hellman (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

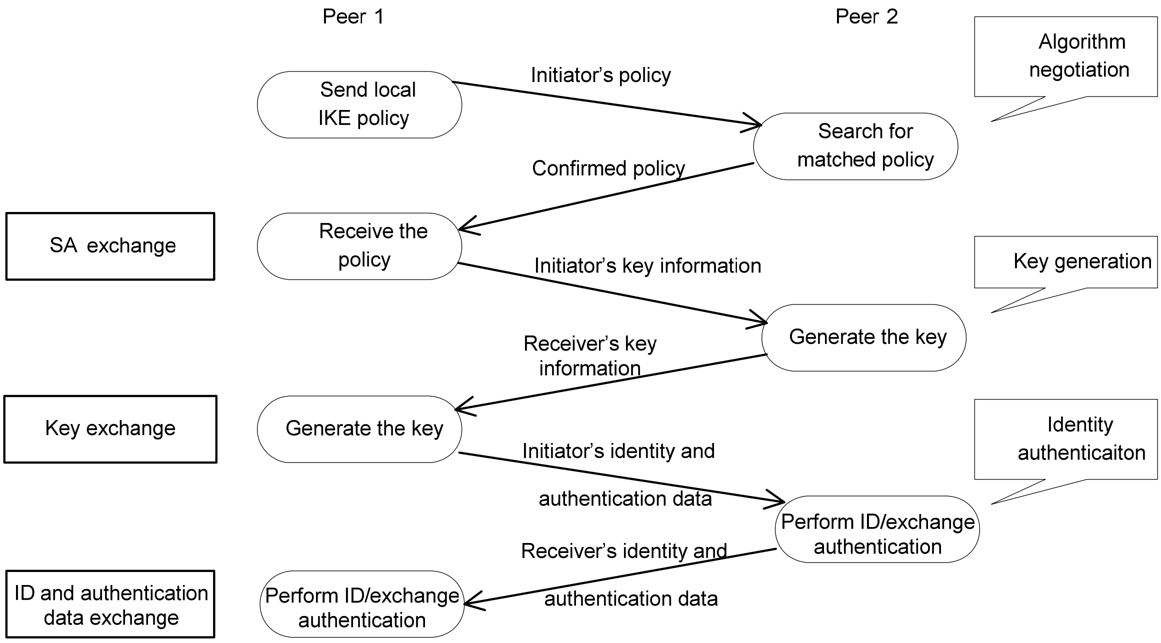
The Perfect Forward Secrecy (PFS) feature is a security feature based on the DH algorithm. By making sure keys have no derivative relations, it guarantees a broken key brings no threats to other keys. For IPsec, PFS is implemented by adding an additional key exchange at IKE negotiation phase 2.

IKE operation

IKE negotiates keys and establishes SAs for IPsec in two phases:

1. Phase 1—The two peers establish an ISAKMP SA, a secure, authenticated channel for communication.
2. Phase 2—Using the ISAKMP SA established in phase 1, the two peers negotiate to establish IPsec SAs.

Figure 55 IKE exchange process in main mode


Peer 1
Peer 2
Algorithm negotiation
Send local IKE policy
Initiator's policy
Search for matched policy
Confirmed policy
SA exchange
Receive the policy
Initiator's key information
Key generation
Generate the key
Receiver's key information
Key exchange
Generate the key
Initiator's identity and authentication data
Identity authenticaiton
Perform ID/exchange authentication
Receiver's identity and authentication data
ID and authentication data exchange
Perform ID/exchange authentication

As shown in Figure 55, the main mode of IKE negotiation in phase 1 involves three pairs of messages:

- SA exchange, used for negotiating the security policy.
- Key exchange, used for exchanging the Diffie-Hellman public value and other values like the random number. Key data is generated in this stage.
- ID and authentication data exchange, used for identity authentication and authentication of data exchanged in phase 1.

IKE functions

IKE provides the following functions for IPsec:

- Automatically negotiates IPsec parameters such as the keys.
- Performs DH exchange when establishing an SA, making sure that each SA has a key independent of other keys.
- Automatically negotiates SAs when the sequence number in the AH or ESP header overflows, making sure that IPsec provides the anti-replay service normally by using the sequence number.
- Provides end-to-end dynamic authentication.
- Identity authentication and management of peers influence IPsec deployment. A large-scale IPsec deployment needs the support of certificate authorities (CAs) or other institutes which manage identity data centrally.

Relationship between IKE and IPsec

Figure 56 Relationship between IKE and IPsec

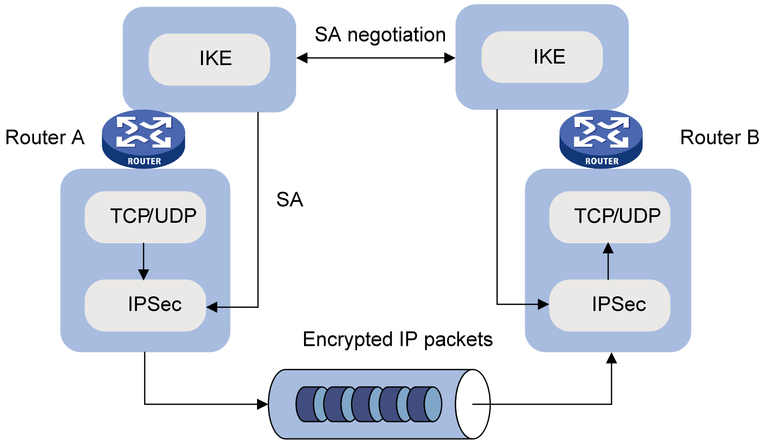


Figure 56 illustrates the relationship between IKE and IPsec:

- IKE is an application layer protocol using UDP and functions as the signaling protocol of IPsec.
- IKE negotiates SAs for IPsec and delivers negotiated parameters and generated keys to IPsec.
- IPsec uses the SAs set up through IKE negotiation for encryption and authentication of IP packets.

Protocols and standards

These protocols and standards are relevant to IKE:

- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*
- RFC 2412, *The OAKLEY Key Determination Protocol*

IKE configuration task list

Prior to IKE configuration, you must determine the following parameters:

- The strength of the algorithms for IKE negotiation (the security protection level), including the identity authentication method, encryption algorithm, authentication algorithm, and DH group. Different algorithms provide different levels of protection. A stronger algorithm means more resistant to decryption of protected data but requires more resources. Generally, the longer the key, the stronger the algorithm.
- The pre-shared key or the PKI domain the certificate belongs to. For more information about PKI configuration, see the chapter "PKI configuration."

To configure IKE:

Task	Remarks
Configuring a name for the local security gateway	Optional.
Configuring an IKE proposal	Optional. Required if you want to specify an IKE proposal for an IKE peer to reference.

Task	Remarks
Configuring an IKE peer	Required.
Setting keepalive timers	Optional.
Setting the NAT keepalive timer	Optional.
Configuring a DPD detector	Optional.
Disabling next payload field checking	Optional.

Configuring a name for the local security gateway

If the IKE negotiation peer uses the security gateway name as its ID to initiate IKE negotiation (the **id-type name** or **id-type user-fqdn** command is configured on the initiator), configure the **ike local-name** command in system view or the **local-name** command in IKE peer view on the local device. If you configure both commands, the name configured in IKE peer view is used.

To configure a name for the local security gateway:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure a name for the local security gateway.	**ike local-name** *name*	Optional. By default, the device name is used as the name of the local security gateway.

Configuring an IKE proposal

An IKE proposal defines a set of attributes describing how IKE negotiation should take place. You may create multiple IKE proposals with different preferences. The preference of an IKE proposal is represented by its sequence number, and the lower the sequence number, the higher the preference.

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, and the peer searches its own IKE proposals for a match. The search starts from the one with the lowest sequence number and proceeds in the ascending order of sequence number until a match is found or all the IKE proposals are found mismatching. The matching IKE proposals will be used to establish the secure tunnel.

Two matching IKE proposals have the same encryption algorithm, authentication method, authentication algorithm, and DH group. The SA lifetime will take the smaller one of the settings on the two sides.

By default, there is an IKE proposal, which has the lowest preference and uses the default encryption algorithm, authentication method, authentication algorithm, DH group, and ISAKMP SA lifetime.

To configure an IKE proposal:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create an IKE proposal and enter its view.	**ike proposal** *proposal-number*	N/A

Step	Command	Remarks
3. Specify an encryption algorithm for the IKE proposal.	**encryption-algorithm aes-cbc** [*key-length*]	Optional. The default is AES-CBC-128.
4. Specify an authentication method for the IKE proposal.	**authentication-method** { **pre-share** | **rsa-signature** }	Optional. Pre-shared key by default.
5. Specify an authentication algorithm for the IKE proposal.	**authentication-algorithm sha**	Optional. SHA1 by default.
6. Specify a DH group for key negotiation in phase 1.	**dh** { **group2** | **group5** | **group14** }	Optional. **group2** (the 1024-bit DH group) by default.
7. Set the ISAKMP SA lifetime for the IKE proposal.	**sa duration** *seconds*	Optional. 86400 seconds by default.

NOTE:

Before an ISAKMP SA expires, IKE negotiates a new SA to replace it. DH calculation in IKE negotiation takes time, especially on low-end devices. To prevent SA updates from influencing normal communication, set the lifetime greater than 10 minutes.

Configuring an IKE peer

For an IPsec policy that uses IKE, you must configure an IKE peer by performing the following tasks:

- Specify the IKE negotiation mode (main mode) for the local end to use in IKE negotiation phase 1. When acting as the IKE negotiation responder, the local end uses the IKE negotiation mode of the remote end.
- Specify the IKE proposals for the local end to use when acting as the IKE negotiation initiator. When acting as the responder, the local end uses the IKE proposals configured in system view for negotiation.
- Configure a pre-shared key for pre-shared key authentication or a PKI domain for digital signature authentication.
- Specify the ID type for the local end to use in IKE negotiation phase 1. With pre-shared key authentication, the ID type must be IP address for main mode IKE negotiation.
- Specify the name or IP address of the local security gateway. You perform this task only when you want to specify a special address, for example, a loopback interface address, as the local security gateway address.
- Specify the name or IP address of the remote security gateway. For the local end to initiate IKE negotiation, you must specify the name or IP address of the remote security gateway on the local end so the local end can find the remote end.
- Enable NAT traversal. If there is NAT gateway on the path for tunneling, you must configure NAT traversal at the two ends of the IPsec tunnel, because one end may use a public address while the other end uses a private address.
- Specify the dead peer detection (DPD) detector for the IKE peer.

To configure an IKE peer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IKE peer and enter IKE peer view.	**ike peer** *peer-name*	N/A
3. Specify the IKE negotiation mode for phase 1.	**exchange-mode main**	Optional. The default is **main**.
4. Specify the IKE proposals for the IKE peer to reference.	**proposal** *proposal-number*&<1-6>	Optional. By default, an IKE peer references no IKE proposals, and, when initiating IKE negotiation, it uses the IKE proposals configured in system view.
5. Configure the pre-shared key for pre-shared key authentication.	**pre-shared-key** [**cipher** | **simple**] *key*	Configure either command according to the authentication method for the IKE proposal.
6. Configure the PKI domain for digital signature authentication.	**certificate domain** *domain-name*	
7. Select the ID type for IKE negotiation phase 1.	**id-type** { **ip** | **name** | **user-fqdn** }	Optional. **ip** by default.
8. Configure the names of the two ends.	• Specify a name for the local security gateway: **local-name** *name* • Configure the name of the remote security gateway: **remote-name** *name*	Optional. By default, no name is configured for the local security gateway in IKE peer view, and the security gateway name configured by using the **ike local-name** command is used. The remote gateway name configured with **remote-name** command on the local gateway must be identical to the local name configured with the **local-name** command on the peer.
9. Configure the IP addresses of the two ends.	• Specify an IP address for the local gateway: **local-address** *ip-address* • Configure the IP addresses of the remote gateway: **remote-address** { *hostname* [**dynamic**] | *low-ip-address* [*high-ip-address*] }	Optional. By default, it is the primary IP address of the interface referencing the security policy. The remote IP address configured with the **remote-address** command on the local gateway must be identical to the local IP address configured with the **local-address** command on the peer.
10. Enable the NAT traversal function for IPsec/IKE.	**nat traversal**	Optional. Disabled by default.

Step	Command	Remarks
11. Apply a DPD detector to the IKE peer.	**dpd** *dpd-name*	Optional. No DPD detector is applied to an IKE peer by default. For more information about DPD configuration, see "Configuring a DPD detector."

NOTE:

After modifying the configuration of an IPsec IKE peer, execute the **reset ipsec sa** and **reset ike sa** commands to clear existing IPsec and IKE SAs. Otherwise, SA re-negotiation will fail.

Setting keepalive timers

IKE maintains the link status of an ISAKMP SA by keepalive packets. Generally, if the peer is configured with the keepalive timeout, you must configure the keepalive packet transmission interval on the local end. If the peer receives no keepalive packet during the timeout interval, the ISAKMP SA will be tagged with the TIMEOUT tag (if it does not have the tag), or be deleted along with the IPsec SAs it negotiated (when it has the tag already).

To set the keepalive timers:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the ISAKMP SA keepalive interval.	**ike sa keepalive-timer interval** *seconds*	No keepalive packet is sent by default.
3. Set the ISAKMP SA keepalive timeout.	**ike sa keepalive-timer timeout** *seconds*	No keepalive packet is sent by default.

NOTE:

The keepalive timeout configured at the local end must be longer than the keepalive interval configured at the remote end. Since it seldom occurs that more than three consecutive packets are lost on a network, the keepalive timeout can be configured to be three times of the keepalive interval.

Setting the NAT keepalive timer

If IPsec traffic needs to pass through NAT security gateways, you must configure the NAT traversal function. If no packet travels across an IPsec tunnel in a certain period of time, the NAT mapping may get aged and be deleted, disabling the tunnel beyond the NAT gateway from transmitting data to the intended end. To prevent NAT mappings from being aged, an ISAKMP SA behind the NAT security gateway sends NAT keepalive packets to its peer at a certain interval to keep the NAT session alive.

To set the NAT keepalive timer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step		Command	Remarks
2.	Set the NAT keepalive interval.	**ike sa nat-keepalive-timer interval** *seconds*	20 seconds by default.

Configuring a DPD detector

Dead peer detection (DPD) irregularly detects dead IKE peers. It works as follows:

1. When the local end sends an IPsec packet, it checks the time the last IPsec packet was received from the peer.
2. If the time interval exceeds the DPD interval, it sends a DPD hello to the peer.
3. If the local end receives no DPD acknowledgement within the DPD packet retransmission interval, it retransmits the DPD hello.
4. If the local end still receives no DPD acknowledgement after having made the maximum number of retransmission attempts (two by default), it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.

DPD enables an IKE entity to check the liveliness of its peer only when necessary. It generates less traffic than the keepalive mechanism, which exchanges messages periodically.

To configure a DPD detector:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a DPD detector and enter its view.	**ike dpd** *dpd-name*	N/A
3.	Set the DPD interval.	**interval-time** *interval-time*	Optional. 10 seconds by default.
4.	Set the DPD packet retransmission interval.	**time-out** *time-out*	Optional. 5 seconds by default.

Disabling next payload field checking

The Next payload field is in the generic payload header of the last payload of the IKE negotiation message (the message comprises multiple payloads). According to the protocol, this field must be 0 if the payload is the last payload of the packet. However, it may be set to other values on some brands of devices. For interoperability, disable the checking of this field.

To disable Next payload field checking:

Step	Command	Remark
Enter system view.	**system-view**	N/A
Disable Next payload field checking.	**ike next-payload check disabled**	Enabled by default.

Displaying and maintaining IKE

Task	Command	Remarks
Display IKE DPD information	**display ike dpd** [*dpd-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IKE peer information	**display ike peer** [*peer-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IKE SA information	**display ike sa** [**verbose** [**connection-id** *connection-id* | **remote-address** *remote-address*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display IKE proposal information	**display ike proposal** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Clear SAs established by IKE	**reset ike sa** [*connection-id*]	Available in user view.

IKE configuration example

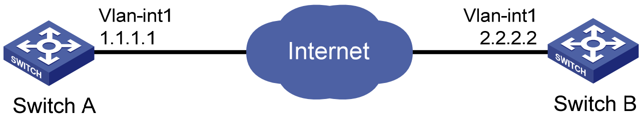
Network requirements

As shown in Figure 57, configure an IPsec tunnel that uses IKE negotiation between gateways Switch A and Switch B to secure the communication between the two switches.

For Switch A, configure an IKE proposal that uses the sequence number 10 and the authentication algorithm SHA1. Configure Switch B to use the default IKE proposal.

Configure the two routers to use the pre-shared key authentication method.

Figure 57 Network diagram



Configuration procedure

1. Make sure Switch A and Switch B can reach each other.
2. 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 ACL 3101 to identify traffic from Switch A to 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
[SwitchA-acl-adv-3101] quit
```

# Create IPsec proposal **tran1**.

```
[SwitchA] ipsec proposal tran1
```

# Set the packet encapsulation mode to tunnel.

```
[SwitchA-ipsec-proposal-tran1] encapsulation-mode tunnel
```

# Use security protocol ESP.

```
[Switch-ipsec-proposal-tran1] transform esp
```

# Specify encryption and authentication algorithms.

```
[SwitchA-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchA-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchA-ipsec-proposal-tran1] quit
```

# Create an IKE proposal numbered 10.

```
[SwitchA] ike proposal 10
```

# Set the authentication algorithm to **SHA1**.

```
[SwitchA-ike-proposal-10] authentication-algorithm sha
```

# Configure the authentication method as pre-shared key.

```
[SwitchA-ike-proposal-10] authentication-method pre-share
```

# Set the ISAKMP SA lifetime to 5000 seconds.

```
[SwitchA-ike-proposal-10] sa duration 5000
[SwitchA-ike-proposal-10] quit
```

# Create IKE peer **peer**.

```
[SwitchA] ike peer peer
```

# Configure the IKE peer to reference IKE proposal 10.

```
[SwitchA-ike-peer-peer]proposal 10
```

# Set the pre-shared key.

```
[SwitchA-ike-peer-peer] pre-shared-key Ab12<><>
```

# Specify the IP address of the peer security gateway.

```
[SwitchA-ike-peer-peer] remote-address 2.2.2.2
[SwitchA-ike-peer-peer] quit
```

# Create an IPsec policy that uses IKE negotiation.

```
[SwitchA] ipsec policy map1 10 isakmp
```

# Reference IPsec proposal **tran1**.

```
[SwitchA-ipsec-policy-isakmp-map1-10] proposal tran1
```

# Reference ACL 3101 to identify the protected traffic.

```
[SwitchA-ipsec-policy-isakmp-map1-10] security acl 3101
```

# Reference IKE peer **peer**.

```
[SwitchA-ipsec-policy-isakmp-map1-10] ike-peer peer
[SwitchA-ipsec-policy-isakmp-map1-10] quit
```

# Apply the IPsec policy to VLAN-interface 1.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ipsec policy map1
```

3. 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 ACL 3101 to identify traffic from Switch B to 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 proposal **tran1**.

```
[SwitchB] ipsec proposal tran1
```

# Set the packet encapsulation mode to tunnel.

```
[SwitchB-ipsec-proposal-tran1] encapsulation-mode tunnel
```

# Use security protocol ESP.

```
[SwitchB-ipsec-proposal-tran1] transform esp
```

# Specify encryption and authentication algorithms.

```
[SwitchB-ipsec-proposal-tran1] esp encryption-algorithm aes 128
[SwitchB-ipsec-proposal-tran1] esp authentication-algorithm sha1
[SwitchB-ipsec-proposal-tran1] quit
```

# Create an IKE proposal numbered 10.

```
[SwitchB] ike proposal 10
```

# Set the authentication algorithm to **SHA1**.

```
[SwitchB-ike-proposal-10] authentication-algorithm sha
```

# Configure the authentication method as pre-shared key.

```
[SwitchB-ike-proposal-10] authentication-method pre-share
```

# Set the ISAKMP SA lifetime to 5000 seconds.

```
[SwitchB-ike-proposal-10] sa duration 5000
[SwitchB-ike-proposal-10] quit
```

# Create IKE peer **peer**.

```
[SwitchB] ike peer peer
```

# Configure the IKE peer to reference IKE proposal 10.

```
[SwitchB-ike-peer-peer]proposal 10
```

# Set the pre-shared key.

```
[SwitchB-ike-peer-peer] pre-shared-key Ab12<><>
```

# Specify the IP address of the peer security gateway.

```
[SwitchB-ike-peer-peer] remote-address 1.1.1.1
[SwitchB-ike-peer-peer] quit
```

# Create an IPsec policy that uses IKE negotiation.

```
[SwitchB] ipsec policy use1 10 isakmp
```

# Reference IPsec proposal **tran1**.

```
[SwitchB-ipsec-policy-isakmp-use1-10] proposal tran1
```

# Reference ACL 3101 to identify the protected traffic.

```
[SwitchB-ipsec-policy-isakmp-use1-10] security acl 3101
```

# Reference IKE peer **peer**.

```
[SwitchB-ipsec-policy-isakmp-use1-10] ike-peer peer
```

```
[SwitchB-ipsec-policy-isakmp-use1-10] quit
```

# Apply the IPsec policy to VLAN-interface 1.

```
[SwitchB-Vlan-interface1] ipsec policy use1
```

Verifying the configuration

After the above configuration, send traffic from Switch B to Switch A. Switch A starts IKE negotiation with Switch B when receiving the first packet. IKE proposal matching starts with the one having the highest priority. During the matching process, lifetime is not involved but it is determined by the IKE negotiation parties.

Troubleshooting IKE

When you configure parameters to establish an IPsec tunnel, enable IKE error debugging to locate configuration problems:

```
<Switch> debugging ike error
```

Invalid user ID

Symptom

Invalid user ID.

Analysis

In IPsec, user IDs are used to identify data flows and to set up different IPsec tunnels for different data flows. Now, the IP address and username are used as the user ID.

The following is the debugging information:

```
got NOTIFY of type INVALID_ID_INFORMATION
```

Or

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

Solution

Check that the ACLs in the IPsec policies configured on the interfaces at both ends are compatible. Configure the ACLs to mirror each other. For more information about ACL mirroring, see the chapter "IPsec configuration."

Proposal mismatch

Symptom

The proposals mismatch.

Analysis

The following is the debugging information:

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

Or

```
drop message from A.B.C.D due to notification type NO_PROPOSAL_CHOSEN
```

The two parties in the negotiation have no matched proposals.

Solution

For the negotiation in phase 1, look up the IKE proposals for a match. For the negotiation in phase 2, check whether the parameters of the IPsec policies applied on the interfaces are matched, and whether the referred IPsec proposals have a match in protocol, encryption and authentication algorithms.

Failing to establish an IPsec tunnel

Symptom

The expected IPsec tunnel cannot be established.

Analysis

Sometimes this may happen that an IPsec tunnel cannot be established or there is no way to communicate in the presence of an IPsec tunnel in an unstable network. According to examination results, however, ACLs of both parties are configured correctly, and proposals are also matched.

In this case, the problem is usually caused by the reboot of one router after the IPsec tunnel is established.

Solution

- Use the **display ike sa** command to check whether both parties have established an SA in phase 1.
- Use the **display ipsec sa policy** command to check whether the IPsec policy on the interface has established IPsec SA.
- If the two commands show that one party has an SA but the other does not, use the **reset ipsec sa** command to clear the IPsec SA that has no corresponding SA, use the **reset ike sa** command to clear the IKE SA that has no corresponding IKE SA, and trigger SA re-negotiation.

ACL configuration error

Symptom

ACL configuration error results in data flow blockage.

Analysis

When multiple devices create different IPsec tunnels early or late, a device may have multiple peers. If the device is not configured with ACL rule, the peers send packets to it to set up different IPsec tunnels in different protection granularity respectively. As the priorities of IPsec tunnels are determined by the order they are established, a device cannot interoperate with other peers in fine granularity when its outbound packets are first matched with an IPsec tunnel in coarse granularity.

Solution

When a device has multiple peers, configure ACLs on the device to distinguish different data flows and try to avoid configuring overlapping ACL rules for different peers. If it is unavoidable, the subrules in fine granularity should be configured with higher preferences.

Configuring SSH2.0

Overview

Secure Shell (SSH) offers an approach to logging in to a remote device securely. Using encryption and strong authentication, SSH protects devices against attacks such as IP spoofing and plain text password interception.

The switch can not only work as an SSH server to support connections with SSH clients, but also work as an SSH client to allow users to establish SSH connections with a remote device acting as the SSH server.

When acting as an SSH server, the switch supports SSH2.0 and SSH1 in non-FIPS mode and supports SSH2 in FIPS mode. When acting as an SSH client, the switch supports SSH2.0 only.

Unless otherwise noted, SSH in this document refers to SSH2.0.

SSH operation

To establish an SSH connection and communicate with each other through the connection, an SSH client and the SSH server go through the stages listed in Table 15.

Table 15 Stages in session establishment and interaction between an SSH client and the server

Stages	Description
Version negotiation	SSH1 and SSH2.0 are supported. The two parties negotiate a version to use.
Key and algorithm negotiation	SSH supports multiple algorithms. The two parties negotiate algorithms for communication, and use the DH key exchange algorithm to generate the same session key and session ID.
Authentication	The SSH server authenticates the client in response to the client's authentication request.
Session request	After passing authentication, the client sends a session request to the server.
Interaction	After the server grants the request, the client and the server start to communicate with each other.

Version negotiation

1. The server opens port 22 to listen to connection requests from clients.
2. The client sends a TCP connection request to the server.
3. After the TCP connection is established, the server sends a packet that carries a version information string to the client. The version information string is in the format SSH-<primary protocol version number>.<secondary protocol version number>-<software version number>. The primary and secondary protocol version numbers constitute the protocol version number. The software version number is used for debugging.
4. After receiving the packet, the client resolves the packet and compares the server's protocol version number with that of its own. If the server's protocol version is lower and supportable, the client uses the protocol version of the server; otherwise, the client uses its own protocol version. In

either case, the client sends a packet to the server to notify the server of the protocol version that it decides to use.

5. The server compares the version number carried in the packet with that of its own. If the server supports the version, the negotiation succeeds and the server and the client proceed with key and algorithm negotiation. Otherwise, the negotiation fails, and the server breaks the TCP connection.

NOTE:

All the packets involved in the preceding steps are transferred in plain text.

Key and algorithm negotiation

IMPORTANT:

Before the key and algorithm negotiation, the server must have already generated a DSA or RSA key pair, which is used in generating the session key and session ID, and by the client to authenticate the identity of the server. For more information about DSA and RSA key pairs, see "Managing public keys."

The server and the client send algorithm negotiation packets to each other, notifying the peer of the supported public key algorithms, encryption algorithms, Message Authentication Code (MAC) algorithms, and compression algorithms.

Based on the received algorithm negotiation packets, the server and the client figure out the algorithms to be used. If the negotiation of any type of algorithm fails, the algorithm negotiation fails and the server tears down the connection with the client.

The server and the client use the DH key exchange algorithm and parameters such as the host key pair to generate the session key and session ID, and the client authenticates the identity of the server.

Through the steps, the server and the client get the same session key and session ID. The session key will be used to encrypt and decrypt data exchanged between the server and client later. The session ID will be used to identify the session established between the server and client and will be used in the authentication stage.

Authentication

SSH supports the following authentication methods:

- **Password authentication**—The SSH server uses AAA for authentication of the client. During password authentication, the SSH client encrypts its username and password, encapsulates them into a password authentication request, and sends the request to the server. After receiving the request, the SSH server decrypts the username and password, checks the validity of the username and password locally or by a remote AAA server, and then informs the client of the authentication result. If the remote AAA server requires the user for a password re-authentication, it carries a prompt in the authentication response sent to the client. The prompt is transparently transmitted to the client, and displayed on the client to notify the user to enter a specified password. After the user enters the correct password and passes validity check on the remote AAA server, the server returns an authentication success message to the client.
- **Publickey authentication**—The server authenticates the client by the digital signature. During publickey authentication, the client sends the server a publickey authentication request that contains its username, public key, and publickey algorithm information. The server checks whether the public key is valid. If the public key is invalid, the authentication fails. Otherwise, the server authenticates the client by the digital signature. Finally, the server sends a message to the client to inform it of the authentication result. The switch supports using the publickey algorithms RSA and DSA for digital signature.

An SSH2.0 server might require the client to pass both password authentication and publickey authentication or either of them. However, if the client is running SSH1, the client only needs to pass either authentication, regardless of the requirement of the server.

The following gives the steps of the authentication stage:

1. The client sends the server an authentication request that includes the username, the authentication method, and the information related to the authentication method (for example, the password in the case of password authentication).
2. The server authenticates the client. If the authentication fails, the server sends the client a message to inform the client of the failure and the methods available for re-authentication.
3. The client selects a method from the list to initiate another authentication.
4. The preceding process repeats until the authentication succeeds or the number of failed authentication attempts exceeds the maximum of authentication attempts. In the latter case, the server tears the session down.

NOTE:

Only clients running SSH2.0 or a later version support password re-authentication that is initiated by the switch acting as the SSH server.

Session request

After passing authentication, the client sends a session request to the server, and the server listens to and processes the request from the client. If the server successfully processes the request, the server sends an SSH_SMSG_SUCCESS packet to the client and goes on to the interaction stage with the client. Otherwise, the server sends an SSH_SMSG_FAILURE packet to the client to indicate that the processing has failed or it cannot resolve the request.

Interaction

In this stage, the server and the client exchanges data as follows:

1. The client encrypts and sends the command to be executed to the server.
2. The server decrypts and executes the command, and then encrypts and sends the result to the client.
3. The client decrypts and displays the result on the terminal.

In the interaction stage, you can paste commands in text format and execute them at the CLI. The text pasted at one time must be within 2000 bytes. HP recommends you to paste commands in the same view. Otherwise, the server might not be able to execute the commands correctly.

To execute commands of more than 2000 bytes, save the commands in configuration file, upload it to the server through Secure FTP (SFTP), and use it to restart the server.

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.

Configuring the switch as an SSH server

SSH server configuration task list

Task	Remarks
Generating DSA or RSA key pairs	Optional
Enabling the SSH server function	Required
Configuring the user interfaces for SSH clients	Required
Configuring a client public key	Required for publickey authentication users and optional for password authentication users
Configuring an SSH user	Optional
Setting the SSH management parameters	Optional
Setting the DSCP value for packets sent by the SSH server	Optional

Generating DSA or RSA key pairs

In the key and algorithm negotiation stage, the DSA or RSA key pairs are used to generate the session key and session ID and for the client to authenticate the server.

Configuration guidelines

- To support SSH clients that use different types of key pairs, generate both DSA and RSA key pairs on the SSH server.
- When an SSH user logs in to the switch, RSA key pairs can be automatically generated if no local DSA or RSA key pairs are configured on the switch.
- The **public-key local create rsa** command generates a server RSA key pair and a host RSA key pair. Each of the key pairs consists of a public key and a private key. The public key in the server key pair of the SSH server is used in SSH1 to encrypt the session key for secure transmission of the key. As SSH2.0 uses the DH algorithm to generate the session key on the SSH server and client, no session key transmission is required in SSH2.0 and the server key pair is not used.
- The **public-key local create dsa** command generates only the host key pair. SSH1 does not support the DSA algorithm.
- For more information about the **public-key local create** command, see *Security Command Reference*.

Configuration procedure

To generate DSA or RSA key pairs on the SSH server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Generate DSA or RSA key pairs.	**public-key local create** { **dsa** | **rsa** }	By default, neither DSA nor RSA key pairs exist.

Enabling the SSH server function

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the SSH server function.	**ssh server enable**	Disabled by default

NOTE:

When the device acts as an SCP server, only one SCP user is allowed to access to the SCP server at one time.

Configuring the user interfaces for SSH clients

An SSH client accesses the switch through a VTY user interface. You must configure the user interfaces for SSH clients to allow SSH login. The configuration takes effect only for clients that log in after the configuration.

Configuration guidelines

- If you configure a user interface to support SSH, be sure to configure the corresponding authentication mode with the **authentication-mode scheme** command.
- For a user interface configured to support SSH, you cannot change the authentication mode. To change the authentication mode, undo the SSH support configuration first.

Configuration procedure

To configure the protocols for a user interface to support:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter user interface view of one or more user interfaces.	**user-interface vty** *number* [*ending-number*]	N/A
3.	Set the login authentication mode to **scheme.**	**authentication-mode scheme**	By default, the authentication mode is **password**.
4.	Configure the user interfaces to support SSH login.	**protocol inbound** { **all** | **ssh** }	Optional. All protocols are supported by default.

For more information about the **authentication-mode** and **protocol inbound** commands, see *Fundamentals Command Reference.*

Configuring a client public key

This configuration task is only necessary for SSH users using publickey authentication.

To allow an SSH user to pass publickey authentication and log in to the server, you must configure the client's DSA or RSA host public key on the server, and configure the client to use the corresponding host private key, so that the server uses the digital signature to authenticate the client.

You can manually configure the public key of an SSH client on the server, or import it from the public key file:

- **Configure it manually**—You can type or copy the public key to the SSH server. The public key must have not been converted and be in the Distinguished Encoding Rules (DER) encoding format.
- **Import it from the public key file**—During the import process, the server will automatically convert the public key in the public key file to a string in Public Key Cryptography Standards (PKCS) format, and save it locally. Before importing the public key, you must upload the public key file (in binary) to the server through FTP or TFTP.

NOTE:

HP recommends you to configure a client public key by importing it from a public key file.

For more information about client public key configuration, see "Managing public keys."

Configuring a client public key manually

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter public key view.	**public-key peer** *keyname*	N/A
3. Enter public key code view.	**public-key-code begin**	N/A
4. Configure a client's host public key.	Enter the content of the host public key	Spaces and carriage returns are allowed between characters.
5. Return to public key view and save the configured host public key.	**public-key-code end**	When you exit public key code view, the system automatically saves the public key.
6. Return to system view.	**peer-public-key end**	N/A

Importing a client public key from a public key file

Step	Command
1. Enter system view.	**system-view**
2. Import the public key from a public key file.	**public-key peer** *keyname* **import sshkey** *filename*

Configuring an SSH user

To configure an SSH user that uses publickey authentication, you must perform the procedure in this section.

To configure an SSH user that uses password authentication, whether together with publickey authentication or not, you must configure a local user account by using the **local-user** command for local authentication, or configure an SSH user account on an authentication server, for example, a RADIUS server, for remote authentication. For more information about the **local-user** command, see *Security Command Reference*.

For password-only SSH users, you do not need to perform the procedure in this section to configure them unless you want to use the **display ssh user-information** command to display all SSH users, including the password-only SSH users, for centralized management.

Configuration guidelines

When you perform the procedure in this section to configure an SSH user, follow these guidelines:

You can set the service type to Stelnet, SFTP, and SCP (Secure copy). For more information about Stelnet, see "Overview." For more information about SFTP, see "Configuring SFTP." For more information about SCP, see "Configuring SCP."

- You can enable one of the following authentication modes for the SSH user:
    - **Password**—The user must pass password authentication.
    - **Publickey authentication**—The user must pass publickey authentication.
    - **Password-publickey authentication**—As an SSH2.0 user, the user must pass both password and publickey authentication. As an SSH1 user, the user must pass either password or publickey authentication.
    - **Any**—The user can use either password authentication or publickey authentication.
- If only publickey authentication is used, the command level accessible to the user is set by the **user privilege level** command on the user interface. If password authentication is used, either with or without publickey authentication, the command level accessible to the user is authorized by AAA.
- SSH1 does not support SCP and SFTP. For an SSH1 client, you must set the service type to **stelnet** or **all**.
- For an SCP or SFTP user, the working folder depends on the authentication method:
    - If only password authentication is used, the working folder is authorized by AAA.
    - If publickey authentication is used, either with or without password authentication, the working folder is set by using the **ssh user** command.
- If you change the authentication mode or public key for an SSH user that has been logged in, the change can take effect only at the next login of the user.
- In FIPS mode, the SSH server does not support any authentication and publickey authentication.

Configuration procedure

To configure an SSH user and specify the service type and authentication method:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Create an SSH user, and specify the service type and authentication method.	• For Stelnet users: ○ In non-FIPS mode: **ssh user** *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* } ○ In FIPS mode: **ssh user** *username* **service-type stelnet authentication-type** { **password** | **password-publickey assign publickey** *keyname* } • For all users, SCP or SFTP users: ○ In non-FIPS mode: **ssh user** *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* } ○ In FIPS mode: **ssh user** *username* **service-type** { **all** | **scp** | **sftp** } **authentication-type** { **password** | **password-publickey assign publickey** *keyname* **work-directory** *directory-name* }	Use one of the commands.

Setting the SSH management parameters

SSH management includes:

- Enabling the SSH server to be compatible with SSH1 client
- Setting the RSA server key pair update interval, applicable to users using SSH1 client
- Setting the SSH user authentication timeout period
- Setting the maximum number of SSH authentication attempts

Setting these parameters can help avoid malicious guessing at and cracking of the keys and usernames, securing your SSH connections.

IMPORTANT:

Authentication fails if the number of authentication attempts (including both publickey and password authentication) exceeds that specified in the **ssh server authentication-retries** command.

To set the SSH management parameters:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the SSH server to support SSH1 clients.	**ssh server compatible-ssh1x** [**enable**]	Optional. By default, the SSH server supports SSH1 clients. This command is not available in FIPS mode.

Step		Command	Remarks
3.	Set the RSA server key pair update interval.	**ssh server rekey-interval** *hours*	Optional. By default, the interval is 0, and the RSA server key pair is not updated. This command is not available in FIPS mode.
4.	Set the SSH user authentication timeout period.	**ssh server authentication-timeout** *time-out-value*	Optional. 60 seconds by default.
5.	Set the maximum number of SSH authentication attempts.	**ssh server authentication-retries** *times*	Optional. 3 by default.

Setting the DSCP value for packets sent by the SSH server

A field in an IPv4 or IPv6 header contains 8 bits and is used to identify the service type of an IP packet. In an IPv4 packet, this field is called "Type of Service (ToS)." In an IPv6 packet, this field is called "Traffic class." According to RFC 2474, the ToS field is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved. When a packet is being transmitted, the network devices can identify its DSCP value, and determines the transmission priority of the packet according to the DSCP value.

To set the DSCP value for packets sent by the SSH server:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the DSCP value for packets sent by the SSH server.	• Set the DSCP value for IPv4 packets sent by the SSH server: **ssh server dscp** *dscp-value* • Set the DSCP value for IPv6 packets sent by the SSH server: **ssh server ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value is 16 in IPv4 packets sent by the SSH server and is 0 in IPv6 packets sent by the SSH server.

Configuring the switch as an SSH client

SSH client configuration task list

Task	Remarks
Specifying a source IP address/interface for the SSH client	Optional
Configuring whether first-time authentication is supported	Optional
Establishing a connection between the SSH client and server	Required
Setting the DSCP value for packets sent by the SSH client	Optional

Specifying a source IP address/interface for the SSH client

This configuration task allows you to specify a source IP address or interface for the client to access the SSH server, improving service manageability.

To specify a source IP address or interface for the client:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A

2.	Specify a source IP address or interface for the SSH client.	• Specify a source IPv4 address or interface for the SSH client:
		ssh client source { **ip** *ip-address* | **interface** *interface-type interface-number* }
		• Specify a source IPv6 address or interface for the SSH client:
		ssh client ipv6 source { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }
			Select either approach.
			By default, an SSH client uses the IP address of the outbound interface defined by the route to the SSH server to access the SSH server.

Configuring whether first-time authentication is supported

When the switch acts as an SSH client and connects to the SSH server, you can configure whether the switch supports first-time authentication.

- With first-time authentication, when an SSH client not configured with the server host public key accesses the server for the first time, the user can continue accessing the server, and save the host public key on the client. When accessing the server again, the client will use the saved server host public key to authenticate the server.
- Without first-time authentication, a client not configured with the server host public key will refuse to access the server. To enable the client to access the server, you must configure the server host public key and specify the public key name for authentication on the client in advance.

Enabling the switch to support first-time authentication

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the switch to support first-time authentication.	**ssh client first-time** [**enable**]	Optional. By default, first-time authentication is supported on a client.

Disabling first-time authentication

For successful authentication of an SSH client not supporting first-time authentication, the server host public key must be configured on the client and the public key name must be specified.

To disable first-time authentication:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Disable first-time authentication support.	**undo ssh client first-time**	By default, first-time authentication is supported on a client.
3. Configure the server host public key.	See "Configuring a client public key"	The method for configuring the server host public key on the client is similar to that for configuring client public key on the server.
4. Specify the host public key name of the server.	**ssh client authentication server** *server* **assign publickey** *keyname*	N/A

Establishing a connection between the SSH client and server

Task	Command	Remarks
Establish a connection between the SSH client and the server, and specify the public key algorithm, preferred encryption algorithm, preferred HMAC algorithm and preferred key exchange algorithm.	• For an IPv4 server: ○ In non-FIPS mode: **ssh2** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * ○ In FIPS mode: **ssh2** *server* [*port-number*] [**identity-key rsa** | **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** }] * • For an IPv6 server: ○ In non-FIPS mode: **ssh2 ipv6** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * ○ In FIPS mode: **ssh2 ipv6** *server* [*port-number*] [**identity-key rsa** | **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** }] *	Use one of the commands in user view.

Setting the DSCP value for packets sent by the SSH client

A field in an IPv4 or IPv6 header contains 8 bits and is used to identify the service type of an IP packet. In an IPv4 packet, this field is called "Type of Service (ToS)." In an IPv6 packet, this field is called "Traffic class." According to RFC 2474, the ToS field is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved. When a packet is being transmitted, the network devices can identify its DSCP value, and determines the transmission priority of the packet according to the DSCP value.

To set the DSCP value for packets sent by the SSH client:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for packets sent by the SSH client.	- Set the DSCP value for IPv4 packets sent by the SSH client: **ssh client dscp** *dscp-value* - Set the DSCP value for IPv6 packets sent by the SSH client: **ssh client ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value is 16 in IPv4 packets sent by the SSH client and is 0 in IPv6 packets sent by the SSH client.

Displaying and maintaining SSH

Task	Command	Remarks
Display the source IP address or interface set for the SFTP client.	**display sftp client source** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the source IP address or interface information on an SSH client.	**display ssh client source** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display SSH server status information or session information on an SSH server.	**display ssh server** { **status** | **session** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the mappings between SSH servers and their host public keys on an SSH client.	**display ssh server-info** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about SSH users on an SSH server.	**display ssh user-information** [*username*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the public keys of the local key pairs.	**display public-key local** { **dsa** | **rsa** } **public** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the public keys of the SSH peers.	**display public-key peer** [**brief** | **name** *publickey-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

For more information about the **display public-key local** and **display public-key peer** commands, see *Security Command Reference*.

SSH server configuration examples

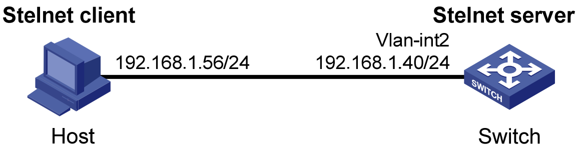
Unless otherwise noted, devices in the configuration examples are operating in non-FIPS mode.

When the switch acts as a server for password authentication

Network requirements

As shown in Figure 58, a host (the SSH client) and a switch (the SSH server) are directly connected. Configure an SSH user on the switch so that the host can securely log in to the switch after passing password authentication. Configure a username and password for the user on the switch.

Figure 58 Network diagram



Configuration procedure

1. Configure the SSH server:

   # Generate the RSA key pairs.

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

   # Generate a DSA key pair.

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

   # Enable the SSH server.

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

   # Configure an IP address for VLAN-interface 1. This address will serve as the destination of the SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

   # Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 15
```

```
[Switch-ui-vty0-15] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit
```

# Create local user **client001**, and set the user command privilege level to 3

```
[Switch] local-user client001
[Switch-luser-client001] password simple aabbcc
[Switch-luser-client001] service-type ssh
[Switch-luser-client001] authorization-attribute level 3
[Switch-luser-client001] quit
```

# Specify the service type for user **client001** as **stelnet**, and the authentication method as **password**. This step is optional.

```
[Switch] ssh user client001 service-type stelnet authentication-type password
```

2. Establish a connection between the SSH client and the SSH server:

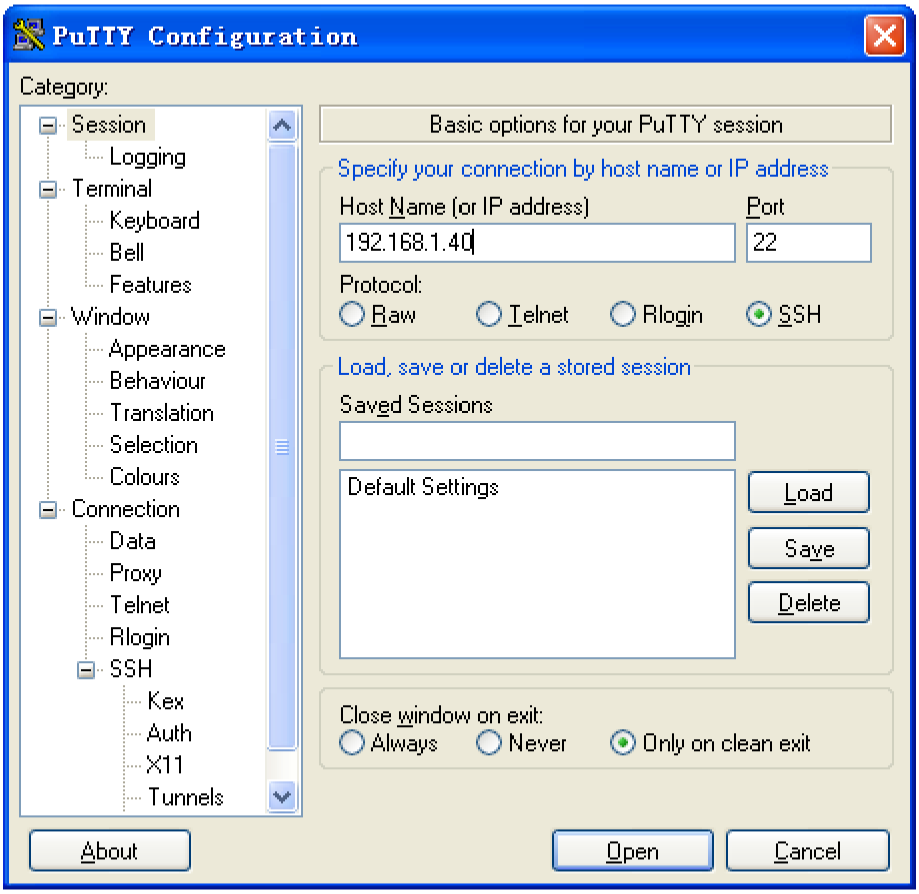
   The switch supports a variety of SSH client software, such as PuTTY, and OpenSSH. The following example uses PuTTY Version 0.58.

   To establish a connection to the SSH server:

   a. Launch PuTTY.exe to enter the interface as shown in Figure 59.

   b. In the **Host Name (or IP address)** text box, enter the IP address of the server 192.168.1.40.

Figure 59 Specifying the host name (or IP address)



Host Name (or IP address): 192.168.1.40

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Close window on exit: ○ Always ○ Never ● Only on clean exit

   c. Click **Open** to connect to the server.

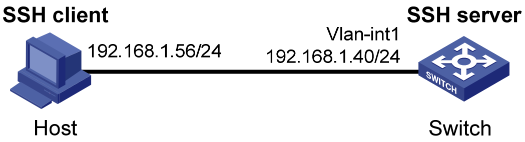
If the connection is normal, you will be prompted to enter the username and password. After entering the username (**client001**) and password (**aabbcc**), you can enter the configuration interface of the server.

When the switch acts as a server for publickey authentication

Network requirements

As shown in Figure 60, a host (the SSH client) and a switch (the SSH server) are directly connected. Configure an SSH user on the switch so that the host can securely log in to the switch after passing publickey authentication. Use the RSA public key algorithm.

Figure 60 Network diagram



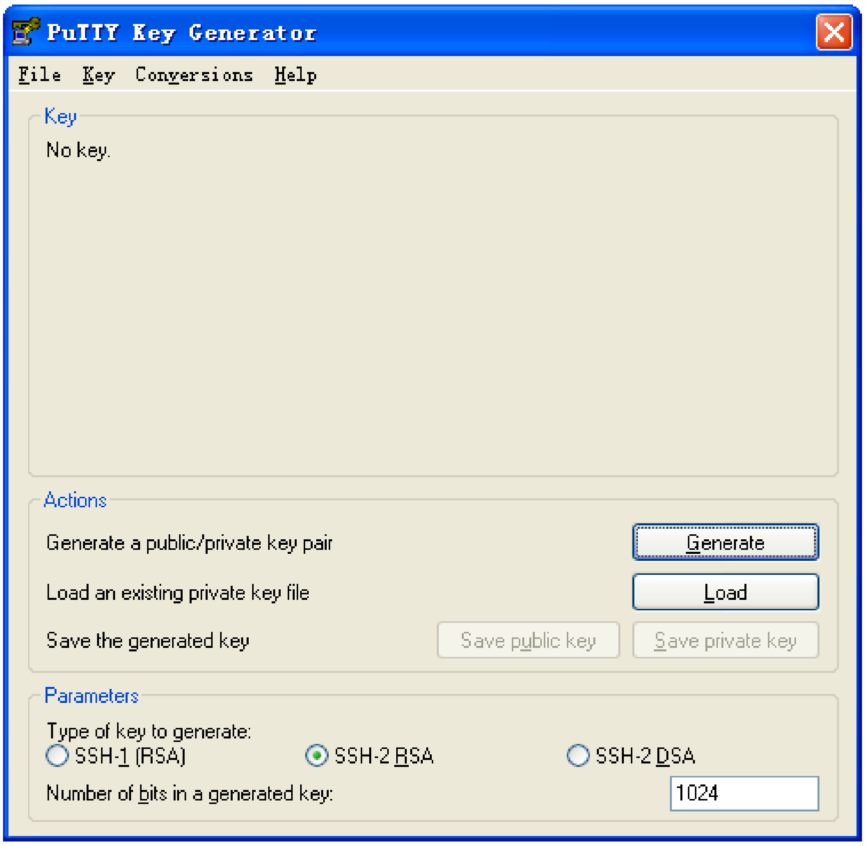
Configuration procedure

During SSH server configuration, the client public key is required. Use the client software to generate RSA key pairs on the client before configuring the SSH server.

1. Generate the RSA key pairs on the SSH client:

   a. Run PuTTYGen.exe, select **SSH-2 RSA** and click **Generate**.

Figure 61 Generating the key pair on the client



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

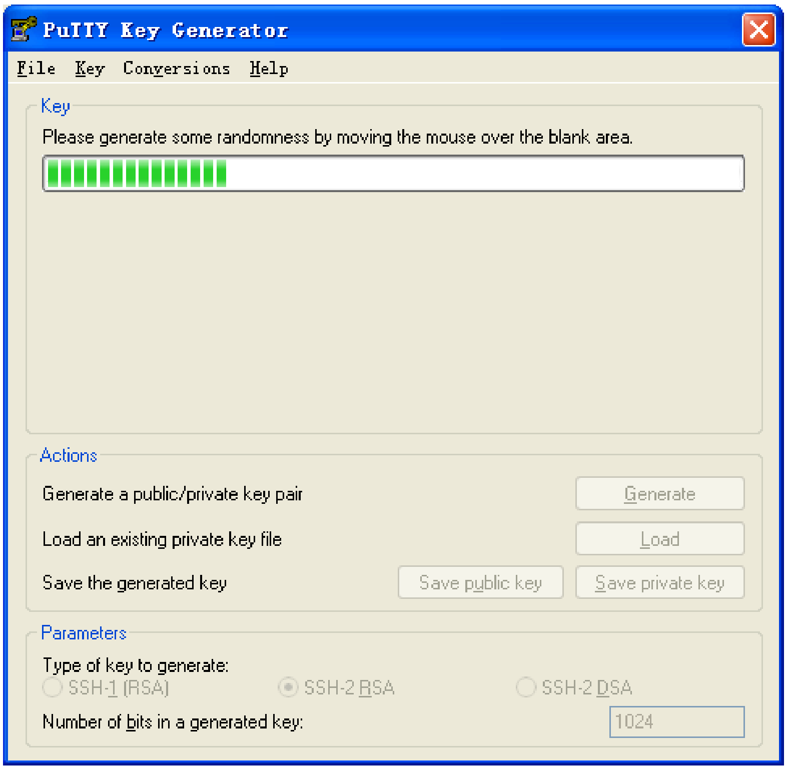
Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

When the generator is generating the key pair, you must move the mouse continuously and keep the mouse off the green progress bar shown in Figure 62. Otherwise, the progress bar stops moving and the key pair generating process will be stopped.

Figure 62 Generating process



Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

Load an existing private key file

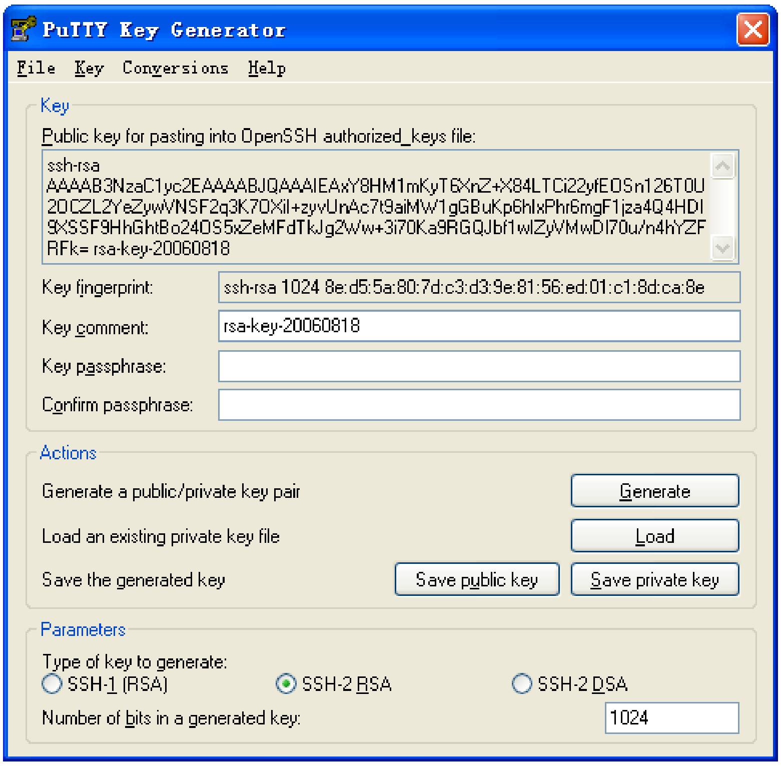
Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

b. After the key pair is generated, click **Save public key** and specify the file name as **key.pub** to save the public key.

Figure 63 Saving the key pair on the client



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAxY8HM1mKyT6XnZ+X84LTCi22yfEOSn126T0U
20CZL2YeZywVNSF2q3K70XiI+zyvUnAc7t9aiMW1gGBuKp6hIxPhr6mgF1jza4Q4HDI
9XSSF9HhGhtBo24OS5xZeMFdTkJg2Ww+3i70Ka9RGQJbf1wIZyVMwDI70u/n4hYZF
RFk= rsa-key-20060818
```

Key fingerprint: ssh-rsa 1024 8e:d5:5a:80:7d:c3:d3:9e:81:56:ed:01:c1:8d:ca:8e

Key comment: rsa-key-20060818

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

c. Click **Save private key** to save the private key.

   A warning window pops up to prompt you whether to save the private key without any protection.

d. Click **Yes** and enter the name of the file for saving the key (**private.ppk** in this case).

e. Transmit the public key file to the server through FTP or TFTP.

2. Configure the SSH server:

   # Generate the RSA key pairs.

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

   # Generate a DSA key pair.

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
```

```
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

# Enable the SSH server.

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

# Configure an IP address for VLAN-interface 1. This address will serve as the destination of the SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

# Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-15] protocol inbound ssh
```

# Set the user command privilege level to 3.

```
[Switch-ui-vty0-15] user privilege level 3
[Switch-ui-vty0-15] quit
```

# Import the client's public key from file **key.pub** and name it **Switch001**.

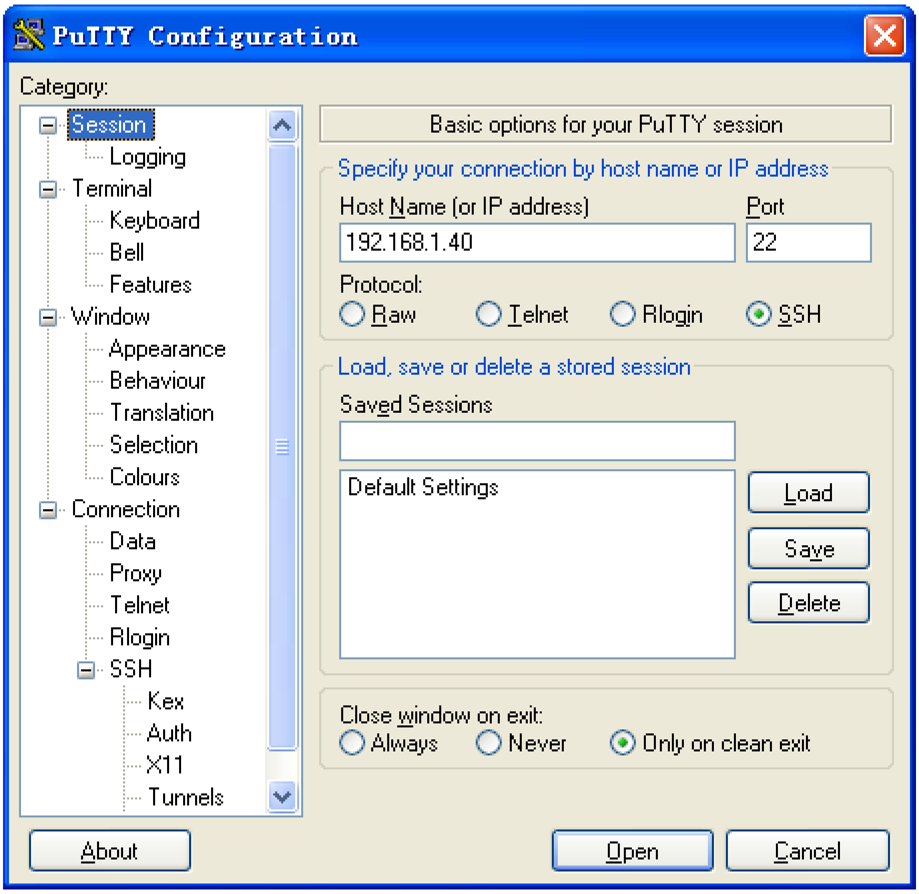
```
[Switch] public-key peer Switch001 import sshkey key.pub
```

# Specify the authentication method for user **client002** as **publickey**, and assign the public key **Switch001** to the user.

```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign
publickey Switch001
```

3. Specify the private key file and establish a connection to the SSH server:
   a. Launch PuTTY.exe to enter the interface as shown in Figure 64.
   b. In the **Host Name (or IP address)** text box, enter the IP address of the server 192.168.1.40.

Figure 64 Specifying the host name (or IP address)



Host Name (or IP address): 192.168.1.40

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

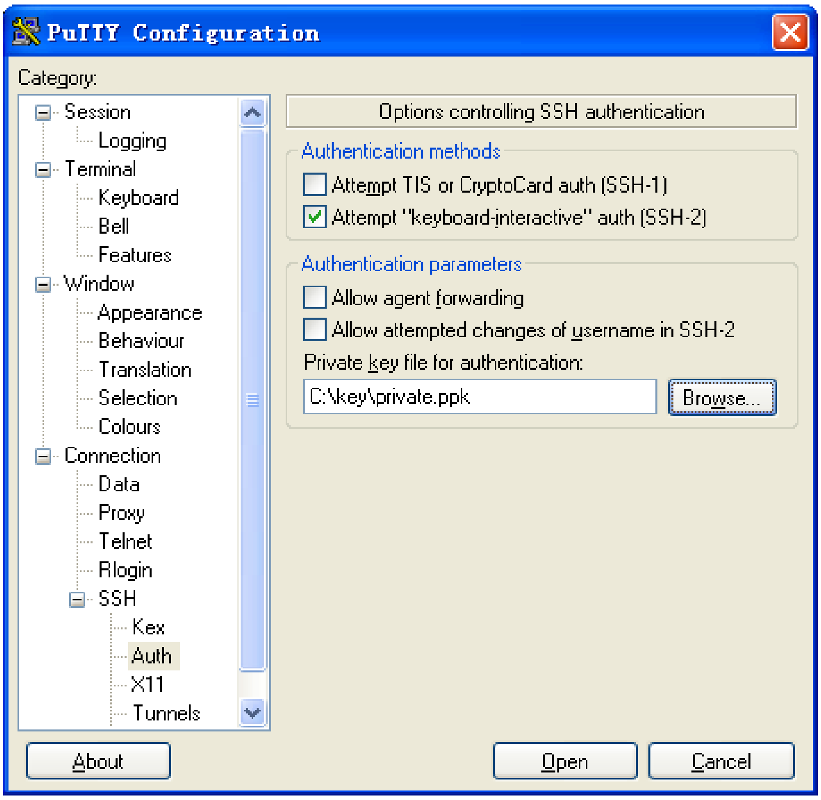
Close window on exit: ○ Always ○ Never ● Only on clean exit

c. Select **Connection** > **SSH** > **Auth** from the navigation tree.

The window as shown in Figure 65 appears.

d. Click **Browse…** to bring up the file selection window, navigate to the private key file (**private.ppk**) and click **OK**.

Figure 65 Specifying the private key file



Options controlling SSH authentication

Authentication methods

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication:

C:\key\private.ppk [Browse...]

e. Click **Open** to connect to the server.

If the connection is normal, you will be prompted to enter the username. After entering the username (**client002**), you can enter the configuration interface of the server.

SSH client configuration examples

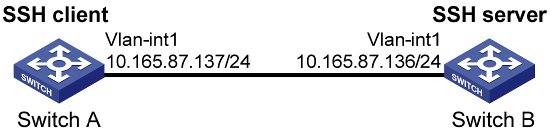
Unless otherwise noted, devices in the configuration examples are operating in non-FIPS mode.

When switch acts as client for password authentication

Network requirements

As shown in Figure 66, Switch A (the SSH client) must pass password authentication to log in to Switch B (the SSH server) through the SSH protocol. Configure the username **client001** and the password **aabbcc** for the SSH client on Switch B.

Figure 66 Network diagram



Configuration procedure

1. Configure the SSH server:

# Generate the RSA key pairs.

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

# Generate a DSA key pair.

```
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

# Enable the SSH server.

```
[SwitchB] ssh server enable
```

# Configure an IP address for VLAN-interface 1, which the SSH client will use as the destination for SSH connection.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

# Set the authentication mode for the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 15
[SwitchB-ui-vty0-15] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-15] protocol inbound ssh
[SwitchB-ui-vty0-15] quit
```

# Create local user **client001**.

```
[SwitchB] local-user client001
[SwitchB-luser-client001] password simple aabbcc
[SwitchB-luser-client001] service-type ssh
[SwitchB-luser-client001] authorization-attribute level 3
[SwitchB-luser-client001] quit
```

# Specify the service type for user **client001** as **stelnet**, and the authentication method as **password**. This step is optional.

```
[SwitchB] ssh user client001 service-type stelnet authentication-type password
```

2. Establish a connection between the SSH client and the SSH server:

# Configure an IP address for VLAN-interface 1.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
[SwitchA] quit
```

# Establish a connection between the SSH client and the SSH server:

- If the client supports first-time authentication, you can directly establish a connection from the client to the server.

  # Establish an SSH connection to server 10.165.87.136.

  ```
  <SwitchA> ssh2 10.165.87.136
  Username: client001
  Trying 10.165.87.136 ...
  Press CTRL+K to abort
  Connected to 10.165.87.136 ...

  The Server is not authenticated. Continue? [Y/N]:y
  Do you want to save the server public key? [Y/N]:n
  Enter password:
  ```

  After you enter the correct password, you can log in to Switch B successfully.

- If the client does not support first-time authentication, perform the following configurations.

  # Disable first-time authentication.

  ```
  [SwitchA] undo ssh client first-time
  ```

  # Configure the host public key of the SSH server. You can get the server host public key by using the **display public-key local dsa public** command on the server.

  ```
  [SwitchA] public-key peer key1
  [SwitchA-pkey-public-key] public-key-code begin
  [SwitchA-pkey-key-code]308201B73082012C06072A8648CE3804013082011F0281810
  0D757262C4584C44C211F18BD96E5F0
  [SwitchA-pkey-key-code]61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE
  65BE6C265854889DC1EDBD13EC8B274
  [SwitchA-pkey-key-code]DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B0
  6FD60FE01941DDD77FE6B12893DA76E
  [SwitchA-pkey-key-code]EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3
  68950387811C7DA33021500C773218C
  [SwitchA-pkey-key-code]737EC8EE993B4F2DED30F48EDACE915F0281810082269009E
  14EC474BAF2932E69D3B1F18517AD95
  [SwitchA-pkey-key-code]94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D02
  492B3959EC6499625BC4FA5082E22C5
  [SwitchA-pkey-key-code]B374E16DD00132CE71B020217091AC717B612391C76C1FB2E
  88317C1BD8171D41ECB83E210C03CC9
  [SwitchA-pkey-key-code]B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC
  9B09EEF0381840002818000AF995917
  [SwitchA-pkey-key-code]E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5D
  F257523777D033BEE77FC378145F2AD
  [SwitchA-pkey-key-code]D716D7DB9FCABB4ADBF6FB4FDB0CA25C761B308EF53009F71
  01F7C62621216D5A572C379A32AC290
  ```

```
[SwitchA-pkey-key-code]E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E
8716261214A5A3B493E866991113B2D
[SwitchA-pkey-key-code]485348
[SwitchA-pkey-key-code] public-key-code end
[SwitchA-pkey-public-key] peer-public-key end
```

# Specify the host public key for the SSH server 10.165.87.136 as **key1**.

```
[SwitchA] ssh client authentication server 10.165.87.136 assign publickey key1
[SwitchA] quit
```

# Establish an SSH connection to server 10.165.87.136.

```
<SwitchA> ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136
Press CTRL+K to abort
Connected to 10.165.87.136...
Enter password:
```

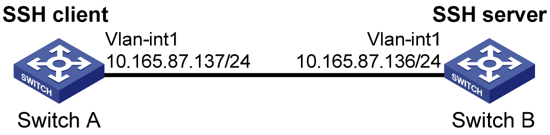
After you enter the correct password, you can log in to Switch B successfully.

When switch acts as client for publickey authentication

Network requirements

As shown in Figure 67, Switch A (the SSH client) must pass publickey authentication to log in to Switch B (the SSH server) through the SSH protocol. Use the DSA public key algorithm.

Figure 67 Network diagram



Configuration procedure

During SSH server configuration, the client public key is required. Use the client software to generate a DSA key pair on the client before configuring the SSH server.

1. Configure the SSH client:

# Create VLAN-interface 1 and assign an IP address to it.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

# Generate a DSA key pair.

```
[SwitchA] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

# Export the DSA public key to file **key.pub**.

```
[SwitchA] public-key local export dsa ssh2 key.pub
[SwitchA] quit
```

Then, transmit the public key file to the server through FTP or TFTP.

2. Configure the SSH server:

# Generate the RSA key pairs.

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

# Generate a DSA key pair.

```
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

# Enable the SSH server.

```
[SwitchB] ssh server enable
```

# Configure an IP address for VLAN-interface 1, which the SSH client will use as the destination for SSH connection.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

# Set the authentication mode for the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 15
[SwitchB-ui-vty0-15] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-15] protocol inbound ssh
```

# Set the user command privilege level to 3.

```
[SwitchB-ui-vty0-15] user privilege level 3
[SwitchB-ui-vty0-15] quit
```

# Import the peer public key from the file **key.pub**.

```
[SwitchB] public-key peer Switch001 import sshkey key.pub
```

Specify the authentication method for user **client002** as **publickey**, and assign the public key **Switch001** to the user.

```
[SwitchB] ssh user client002 service-type stelnet authentication-type publickey
assign publickey Switch001
```

3. Establish an SSH connection to the server 10.165.87.136.

```
<SwitchA> ssh2 10.165.87.136
Username: client002
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

Later, you will find that you have logged in to Switch B successfully.

Configuring SFTP

Overview

The Secure File Transfer Protocol (SFTP) is a new feature in SSH2.0.

SFTP uses the SSH connection to provide secure data transfer. The switch can serve as the SFTP server, allowing a remote user to log in to the SFTP server for secure file management and transfer. The switch can also serve as an SFTP client, enabling a user to log in from the switch to a remote device for secure file transfer.

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.

Configuring the switch as an SFTP server

Before you configure this task, complete the following tasks:

- Configure the SSH server.
- Use the **ssh user service-type** command to set the service type of SSH users to **sftp** or **all**.

For more information about the configuration procedures, see "Configuring SSH2.0."

Enabling the SFTP server

This configuration task will enable the SFTP service so that a client can log in to the SFTP server through SFTP.

When the switch acts as the SFTP server, the following restrictions are imposed on the SFTP client:

- Only one client can access the SFTP server at a time. If the SFTP client uses WinSCP, a file on the server cannot be modified directly. It can only be downloaded to a local place, modified, and then uploaded to the server.
- The user privilege level for the SFTP client must be correctly configured.
    - Set the user privilege level to 3 if the SFTP client executes the following commands: **delete**, **remove**, **rename**, **rmdir**, and **mkdir**.
    - Set the user privilege level to 3 if the SFTP client executes the **put** command and uses the uploaded local file to overwrite the file on the SFTP server.
    - Set the user privilege level to 2 if the SFTP client executes the **put** command and does not use the uploaded local file to overwrite the file on the SFTP server.
    - Set the user privilege level to any value from 0 to 3 if the SFTP client executes other commands.

To enable the SFTP server:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the SFTP server.	**sftp server enable**	Disabled by default.

Configuring the SFTP connection idle timeout period

Once the idle period of an SFTP connection exceeds the specified threshold, the system automatically tears the connection down.

To configure the SFTP connection idle timeout period:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the SFTP connection idle timeout period.	**sftp server idle-timeout** *time-out-value*	Optional. 10 minutes by default.

Configuring the switch as an SFTP client

Specifying a source IP address or interface for the SFTP client

You can configure a client to use only a specified source IP address or interface to access the SFTP server, enhancing the service manageability.

To specify a source IP address or interface for the SFTP client:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A

2.	Specify a source IP address or interface for the SFTP client.	• Specify a source IPv4 address or interface for the SFTP client:
		sftp client source { **ip** *ip-address* | **interface** *interface-type interface-number* }
		• Specify a source IPv6 address or interface for the SFTP client:
		sftp client ipv6 source { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }
			Use either command.
			By default, an SFTP client uses the IP address of the interface specified by the route of the switch to access the SFTP server.

Establishing a connection to the SFTP server

This configuration task will enable the SFTP client to establish a connection to the remote SFTP server and enter SFTP client view.

To enable the SFTP client:

<table>
<tr><th>Task</th><th>Command</th><th>Remarks</th></tr>
<tr><td>Establish a connection to the remote SFTP server and enter SFTP client view.</td><td>• Establish a connection to the remote IPv4 SFTP server and enter SFTP client view:
○ In non-FIPS mode:
sftp *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *
○ In FIPS mode:
sftp ipv6 *server* [*port-number*] [**identity-key rsa** | **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** }] *
• Establish a connection to the remote IPv6 SFTP server and enter SFTP client view:
○ In non-FIPS mode:
sftp ipv6 *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *
○ In FIPS mode:
sftp ipv6 *server* [*port-number*] [**identity-key rsa** | **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** }] *</td><td>Use one of the commands in user view.</td></tr>
</table>

Working with SFTP directories

SFTP directory operations include:

- Changing or displaying the current working directory
- Displaying files under a directory or the directory information
- Changing the name of a directory on the server
- Creating or deleting a directory

To work with the SFTP directories:

Step	Command	Remarks
1. Enter SFTP client view.	For more information, see "Establishing a connection to the SFTP server."	Execute the command in user view.
2. Change the working directory of the remote SFTP server.	**cd** [*remote-path*]	Optional.
3. Return to the upper-level directory.	**cdup**	Optional.
4. Display the current working directory of the remote SFTP server.	**pwd**	Optional.

Step	Command	Remarks
5. Display files under a directory.	- **dir** [**-a** | **-l**] [*remote-path*] - **ls** [**-a** | **-l**] [*remote-path*]	Optional. The **dir** command functions as the **ls** command.
6. Change the name of a directory on the SFTP server.	**rename** *oldname newname*	Optional.
7. Create a new directory on the remote SFTP server.	**mkdir** *remote-path*	Optional.
8. Delete one or more directories from the SFTP server.	**rmdir** *remote-path*&<1-10>	Optional.

Working with SFTP files

SFTP file operations include:

- Changing the name of a file
- Downloading a file
- Uploading a file
- Displaying a list of the files
- Deleting a file

To work with SFTP files:

Step	Command	Remarks
1. Enter SFTP client view.	For more information, see "Establishing a connection to the SFTP server."	Execute the command in user view.
2. Change the name of a file on the SFTP server.	**rename** *old-name new-name*	Optional.
3. Download a file from the remote server and save it locally.	**get** *remote-file* [*local-file*]	Optional.
4. Upload a local file to the remote SFTP server.	**put** *local-file* [*remote-file*]	Optional.
5. Display the files under a directory.	- **dir** [**-a** | **-l**] [*remote-path*] - **ls** [**-a** | **-l**] [*remote-path*]	Optional. The **dir** command functions as the **ls** command.
6. Delete one or more directories from the SFTP server.	- **delete** *remote-file*&<1-10> - **remove** *remote-file*&<1-10>	Optional. The **delete** command functions as the **remove** command.

Displaying help information

This configuration task will display a list of all commands or the help information of an SFTP client command, such as the command format and parameters.

To display a list of all commands or the help information of an SFTP client command:

Step		Command	Remarks
1.	Enter SFTP client view.	For more information, see "Establishing a connection to the SFTP server."	Execute the command in user view.
2.	Display a list of all commands or the help information of an SFTP client command.	**help** [**all** | *command-name*]	N/A

Terminating the connection to the remote SFTP server

Step		Command	Remarks
1.	Enter SFTP client view.	For more information, see "Establishing a connection to the SFTP server."	Execute the command in user view.
2.	Terminate the connection to the remote SFTP server and return to user view.	• **bye** • **exit** • **quit**	Use any of the commands. These three commands function in the same way.

Setting the DSCP value for packets sent by the SFTP client

A field in an IPv4 or IPv6 header contains 8 bits and is used to identify the service type of an IP packet. In an IPv4 packet, this field is called "Type of Service (ToS)." In an IPv6 packet, this field is called "Traffic class." According to RFC 2474, the ToS field is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved. When a packet is being transmitted, the network devices can identify its DSCP value, and determines the transmission priority of the packet according to the DSCP value.

To set the DSCP value for packets sent by the SFTP client:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the DSCP value for packets sent by the SFTP client.	• Set the DSCP value for IPv4 packets sent by the SFTP client: **sftp client dscp** *dscp-value* • Set the DSCP value for IPv6 packets sent by the SFTP client: **sftp client ipv6 dscp** *dscp-value*	Optional. By default, the DSCP value is 16 in IPv4 packets sent by the SFTP client and is 8 in IPv6 packets sent by the SFTP client.

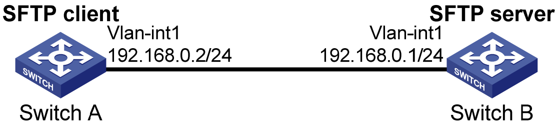
SFTP client configuration example

Unless otherwise noted, devices in the configuration example are operating in non-FIPS mode.

Network requirements

As shown in Figure 68, an SSH connection is required between Switch A and Switch B. Switch A, an SFTP client, needs to log in to Switch B for file management and file transfer. Use publickey authentication and the RSA public key algorithm.

Figure 68 Network diagram



Configuration procedure

During SFTP server configuration, the client public key is required. Use the client software to generate RSA key pairs on the client before configuring the SFTP server.

1. Configure the SFTP client:

   # Create VLAN-interface 1 and assign an IP address to it.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

   # Generate the RSA key pairs.

```
[SwitchA] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

   # Export the host public key to file **pubkey**.

```
[SwitchA] public-key local export rsa ssh2 pubkey
[SwitchA] quit
```

   Then, transmit the public key file to the server through FTP or TFTP.

2. Configure the SFTP server:

   # Generate the RSA key pairs.

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
```

```
++++++++
++++++++++++++
+++++
++++++++
```

# Generate a DSA key pair.

```
[SwitchB] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

# Enable the SSH server.

```
[SwitchB] ssh server enable
```

# Enable the SFTP server.

```
[SwitchB] sftp server enable
```

# Configure an IP address for VLAN-interface 1, which the SSH client uses as the destination for SSH connection.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

# Set the authentication mode on the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 15
[SwitchB-ui-vty0-15] authentication-mode scheme
```

# Set the protocol that a remote user uses to log in as **SSH**.

```
[SwitchB-ui-vty0-15] protocol inbound ssh
[SwitchB-ui-vty0-15] quit
```

# Import the peer public key from the file **pubkey**.

```
[SwitchB] public-key peer Switch001 import sshkey pubkey
```

# For user **client001**, set the service type as SFTP, authentication method as publickey, public key as **Switch001**, and working folder as **flash:/**

```
[SwitchB] ssh user client001 service-type sftp authentication-type publickey assign
publickey Switch001 work-directory flash:/
```

3. Establish a connection between the SFTP client and the SFTP server:

# Establish a connection to the remote SFTP server and enter SFTP client view.

```
<SwitchA> sftp 192.168.0.1 identity-key rsa
Input Username: client001
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
```

```
sftp-client>
```

# Display files under the current directory of the server, delete the file named **z**, and check if the file has been deleted successfully.

```
sftp-client> dir
-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-client> delete z
The following File will be deleted:
/z
Are you sure to delete it? [Y/N]:y
This operation might take a long time.Please wait...

File successfully Removed
sftp-client> dir
-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 named **new1** and check if it has been created successfully.

```
sftp-client> mkdir new1
New directory created
sftp-client> dir
-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
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
```

# Rename directory **new1** to **new2** and check if the directory has been renamed successfully.

```
sftp-client> rename new1 new2
File successfully renamed
sftp-client> dir
-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
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
```

# Download the **pubkey2** file from the server and save it as local file **public**.

```
sftp-client> get pubkey2 public
Remote  file:/pubkey2 --->  Local file: public
Downloading file successfully ended
```

# Upload the local file **pu** to the server, save it as **puk**, and check if the file has been uploaded successfully.

```
sftp-client> put pu puk
Local file:pu --->  Remote file: /puk
Uploading file successfully ended
sftp-client> dir
-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
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
sftp-client>
```

# Terminate the connection to the remote SFTP server.

```
sftp-client> quit
Bye
Connection closed.
<SwitchA>
```

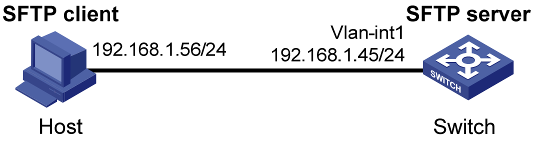
SFTP server configuration example

Unless otherwise noted, devices in the configuration example are operating in non-FIPS mode.

Network requirements

As shown in Figure 69, an SSH connection is required between the host and the switch. The host, an SFTP client, needs to log in to the switch for file management and file transfer. Use password authentication and configure the username **client002** and the password **aabbcc** for the client on the switch.

Figure 69 Network diagram



Configuration procedure

1. Configure the SFTP server:

# Generate the RSA key pairs.

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

# Generate a DSA key pair.

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

# Enable the SSH server.

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

# Enable the SFTP server.

```
[Switch] sftp server enable
```

# Configure an IP address for VLAN-interface 1, which the client will use as the destination for SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
```

# Set the authentication mode of the user interfaces to AAA.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
```

# Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-15] protocol inbound ssh
[Switch-ui-vty0-15] quit
```

# Configure a local user named **client002** with the password being **aabbcc** and the service type being SSH.

```
[Switch] local-user client002
[Switch-luser-client002] password simple aabbcc
[Switch-luser-client002] service-type ssh
[Switch-luser-client002] quit
```

# Configure the user authentication method as **password** and service type as **SFTP**.

```
[Switch] ssh user client002 service-type sftp authentication-type password
```

2. Establish a connection between the SFTP client and the SFTP server:

   The switch supports a variety of SFTP client software. The following example uses PSFTP of PuTTy Version 0.58.

NOTE:

PSFTP supports only password authentication.

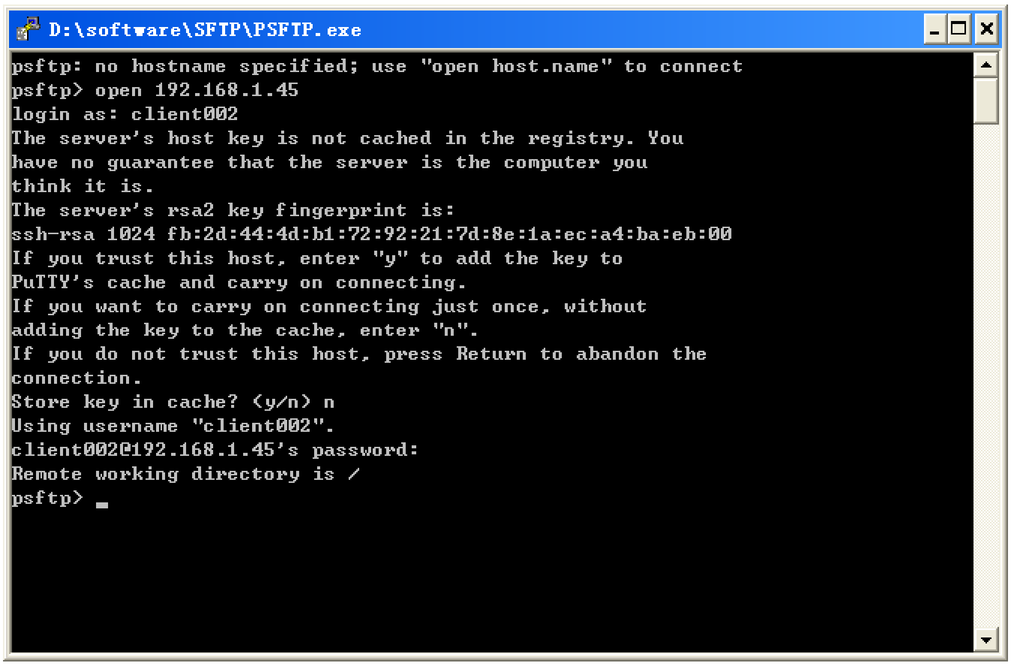
To establish a connection to the remote SFTP server:

a. Run the psftp.exe to launch the client interface as shown in Figure 70, 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.

Figure 70 SFTP client interface



```
psftp: no hostname specified; use "open host.name" to connect
psftp> open 192.168.1.45
login as: client002
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 fb:2d:44:4d:b1:72:92:21:7d:8e:1a:ec:a4:ba:eb:00
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) n
Using username "client002".
client002@192.168.1.45's password:
Remote working directory is /
psftp> _
```

Configuring SCP

Overview

Secure copy (SCP) is based on SSH2.0 and offers a secure approach to copying files.

SCP uses SSH connections for copying files. The switch can act as the SCP server, allowing a user to log in to the switch for file upload and download. The switch can also act as an SCP client, enabling a user to log in from the switch to a remote server for secure file transfer.

NOTE:

When the switch acts as an SCP server, only one of the FTP, SFTP or SCP user can access the switch.

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.

Configuring the switch as an SCP server

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the SSH server.	For more information, see the security guide for your switch.	N/A
3. Create an SSH user for a SCP client, set the service type to **all** or **scp**, and specify the authentication method.	**ssh user** *username* **service-type** { **all** | **scp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }	N/A
4. Create a user account and assign a working directory for the SSH user on the switch or a remote server if password authentication is used.	• On the remote server (Details not shown.) • On the switch: a. **local-user** b. **password** c. **service-type ssh** d. **authorization-attribute work-directory** *directory-name*	Skip this step if publickey authentication, whether with password authentication or not, is used. Make sure that the local user account has the name username as the username specified in the **ssh user** command.

When you set the working directory for the user, follow these guidelines:

- If only password authentication is used, the working directory specified in the **ssh user** command does not take effect. You must set the working directory on the remote server or in the local user account for the SSH user.
- If publickey authentication, whether with password authentication or not, is used, you must set the working directory in the **ssh user** command.

Configuring the switch as the SCP client

To upload or download files to or from an SCP server:

<table>
<tr><th>Step</th><th>Command</th><th>Remarks</th></tr>
<tr><td>1. Upload a file to an SCP server.</td><td>• Upload a file to the IPv4 SCP server:
○ In non-FIPS mode:
scp *server* [*port-number*] **put** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *
○ In FIPS mode:
scp *server* [*port-number*] **put** *source-file-path* [*destination-file-path*] [**identity-key rsa** | **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** }] *
• Upload a file to the IPv6 SCP server:
○ In non-FIPS mode:
scp ipv6 *server* [*port-number*] **put** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *
○ In FIPS mode:
scp ipv6 *server* [*port-number*] **put** *source-file-path* [*destination-file-path*] [**identity-key rsa** | **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** }] *</td><td>Use one of the commands.
Available in user view.</td></tr>
</table>

Step	Command	Remarks
2. Download a file from an SCP server.	- Download a file from the remote IPv4 SCP server: ○ In non-FIPS mode: **scp** *server* [*port-number*] **get** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * ○ In FIPS mode: **scp** *server* [*port-number*] **get** *source-file-path* [*destination-file-path*] [**identity-key rsa** | **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** }] * - Download a file from the remote IPv6 SCP server: ○ In non-FIPS mode: **scp ipv6** *server* [*port-number*] **get** *source-file-path* [*destination-file-path*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] * ○ In FIPS mode: **scp ipv6** *server* [*port-number*] **get** *source-file-path* [*destination-file-path*] [**identity-key rsa** | **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** }] *	

IMPORTANT:

File transfer interruption during a downloading process can result in file fragments on the switch. You must manually delete them.

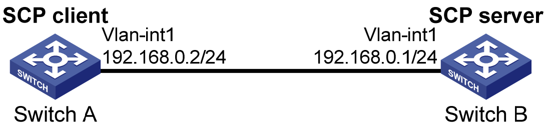
SCP client configuration example

Unless otherwise noted, devices in the configuration example are operating in non-FIPS mode.

Network requirements

As shown in Figure 71, switch A acts as a client and download the file **remote.bin** from switch B. The user has the username **test** and uses the password authentication method.

Figure 71 Network diagram



Configuration procedure

# Create VLAN-interface 1 and assign an IP address to it.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

# Download the file **remote.bin** from the SCP server, save it locally and change the file name to **local.bin**.

```
<SwitchA> scp 192.168.0.1 get remote.bin local.bin
Username: test
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n
Enter password:
18471 bytes transfered in 0.001 seconds.
```

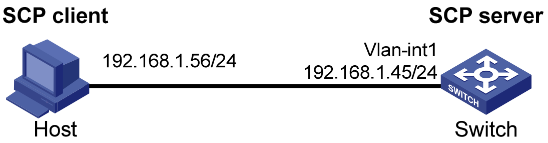
SCP server configuration example

Unless otherwise noted, devices in the configuration example are operating in non-FIPS mode.

Network requirements

As shown in Figure 72, the switch acts as the SCP server, and the host acts as the SCP client. The host establishes an SSH connection to the switch. The user uses the username **test** and the password **aabbcc.** The username and password are saved on the switch for local authentication.

Figure 72 Network diagram



Configuration procedure

# Generate the RSA key pairs.

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++
++++++++++++++
+++++
++++++++
```

# Generate the DSA key pair.

```
[Switch] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++++
```

# Enable the SSH server function.

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

# Configure an IP address for VLAN-interface 1, which the client will use as the destination for SSH connection.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
```

# Set the authentication mode of the user interfaces to AAA.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
```

# Enable the user interfaces to support all protocols including SSH.

```
[Switch-ui-vty0-15] protocol inbound all
[Switch-ui-vty0-15] quit
```

# Create a local user named **test**.

```
[Switch] local-user test
[Switch-luser-test] password simple aabbcc
[Switch-luser-test] service-type ssh
[Switch-luser-test] quit
```

# Configure the SSH user authentication method as **password** and service type as **scp**.

```
[Switch] ssh user test service-type scp authentication-type password
```

Configuring SSL

Overview

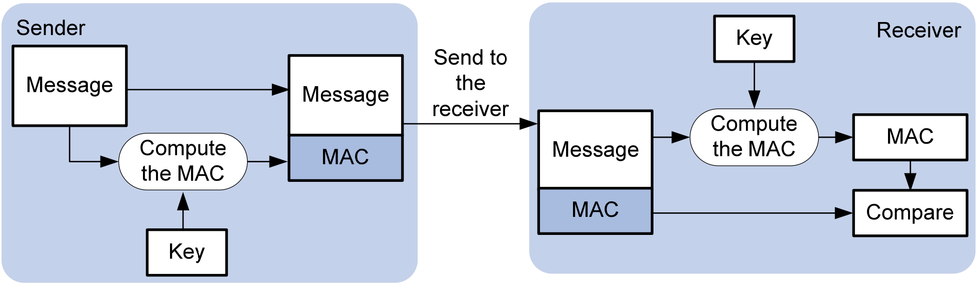
Secure Sockets Layer (SSL) is a security protocol that provides secure connection services for TCP-based application layer protocols such as Hypertext Transfer Protocol (HTTP). It is widely used in e-business and online banking to ensure secure data transmission over the Internet.

SSL security mechanism

Secure connections provided by SSL have these features:

- **Confidentiality**—SSL uses a symmetric encryption algorithm to encrypt data and uses the key exchange algorithm of Rivest, Shamir, and Adelman (RSA) to encrypt the key to be used by the symmetric encryption algorithm.
- **Authentication**—SSL supports certificate-based identity authentication of the server and client by using the digital signatures. The SSL server and client obtain certificates from a certificate authority (CA) through the Public Key Infrastructure (PKI).
- **Reliability**—SSL uses the key-based message authentication code (MAC) to verify message integrity. A MAC algorithm transforms a message of any length to a fixed-length message. With the key, the sender uses the MAC algorithm to compute the MAC value of a message. Then, the sender suffixes the MAC value to the message and sends the result to the receiver. The receiver uses the same key and MAC algorithm to compute the MAC value of the received message, and compares the locally computed MAC value with that received. If the two values match, the receiver considers the message intact; otherwise, the receiver considers that the message has been tampered with in transit and discards the message.

Figure 73 Message integrity verification by a MAC algorithm



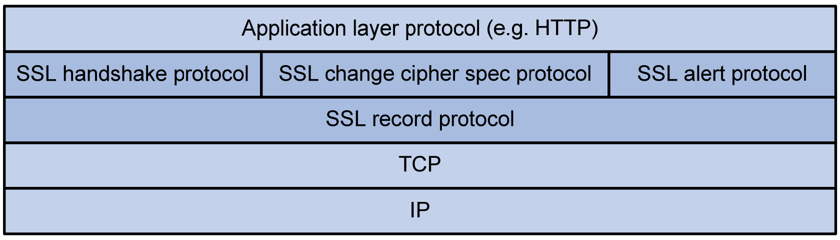
For more information about symmetric key algorithms, asymmetric key algorithm RSA and digital signature, see "Managing public keys."

For more information about PKI, certificate, and CA, see "Configuring PKI."

SSL protocol stack

The SSL protocol consists of two layers of protocols: the SSL record protocol at the lower layer and the SSL handshake protocol, change cipher spec protocol, and alert protocol at the upper layer.

Figure 74 SSL protocol stack


Application layer protocol (e.g. HTTP)
SSL handshake protocol
SSL change cipher spec protocol
SSL alert protocol
SSL record protocol
TCP
IP

- **SSL record protocol**—Fragments data to be transmitted, computes and adds MAC to the data, and encrypts the data before transmitting it to the peer end.
- **SSL handshake protocol**—Negotiates the cipher suite to be used for secure communication (including the symmetric encryption algorithm, key exchange algorithm, and MAC algorithm), securely exchanges the key between the server and client, and implements identity authentication of the server and client. Through the SSL handshake protocol, a session is established between a client and the server. A session consists of a set of parameters, including the session ID, peer certificate, cipher suite, and master secret.
- **SSL change cipher spec protocol**—Used for notification between the client and the server that the subsequent packets are to be protected and transmitted based on the newly negotiated cipher suite and key.
- **SSL alert protocol**—Enables the SSL client and server to send alert messages to each other. 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.

Configuration task list

Task	Remarks
Configuring an SSL server policy	Required
Configuring an SSL client policy	Optional

Configuring an SSL server policy

An SSL server policy is a set of SSL parameters for a server to use when booting up. An SSL server policy takes effect only after it is associated with an application such as HTTPS.

SSL mainly comes in these versions: SSL 2.0, SSL 3.0, and TLS 1.0, where TLS 1.0 corresponds to SSL 3.1. When the switch acts as an SSL server, it can communicate with clients running SSL 3.0 or TLS 1.0, and can identify the SSL 2.0 Client Hello message from a client supporting SSL 2.0 and SSL 3.0/TLS 1.0 and notify the client to use SSL 3.0 or TLS 1.0 to communicate with the server.

To configure an SSL server policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an SSL server policy and enter its view.	**ssl server-policy** *policy-name*	N/A
3. Specify a PKI domain for the SSL server policy.	**pki-domain** *domain-name*	Optional. By default, no PKI domain is specified for an SSL server policy. The SSL server generates a certificate itself instead of requesting one from the CA. After you specify a PKI domain, the SSL server requests a certificate through the PKI domain. If the client requires certificate-based authentication for the SSL server, you must use this command to specify a PKI domain. For more information about PKI domain configuration, see "Configuring PKI."
4. Specify the cipher suites for the SSL server policy to support.	- In non-FIPS mode: **ciphersuite** [**rsa_3des_ede_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: **ciphersuite** [**dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_256_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha**] *	Optional. By default, an SSL server policy supports all cipher suites.
5. Set the handshake timeout time for the SSL server.	**handshake timeout** *time*	Optional. 3600 seconds by default.
6. Set the SSL connection close mode.	**close-mode wait**	Optional. By default, an SSL server sends a close-notify alert message to the client and closes the connection without waiting for the close-notify alert message from the client.
7. Set the maximum number of cached sessions and the caching timeout time.	**session** { **cachesize** *size* | **timeout** *time* } *	Optional. The defaults are as follows: - 500 for the maximum number of cached sessions. - 3600 seconds for the caching timeout time.

Step	Command	Remarks
8. Enable the SSL server to perform digital certificate-based authentication for SSL clients.	**client-verify enable**	Optional. By default, the SSL server does not require clients to be authenticated.
9. Enable SSL client weak authentication.	**client-verify weaken**	Optional. Disabled by default. This command takes effect only when the **client-verify enable** command is configured.

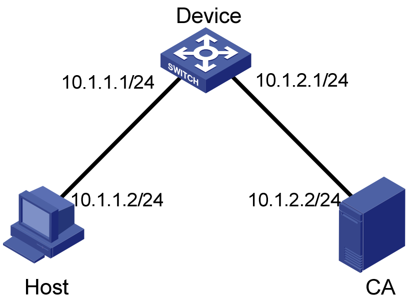
SSL server policy configuration example

Network requirements

As shown in Figure 75, users need to access and control the device through web pages.

For security of the device and to make sure that data is not eavesdropped or tampered with, configure the device so that users must use HTTPS (Hypertext Transfer Protocol Secure, which uses SSL) to log in to the web interface of the device.

Figure 75 Network diagram



Configuration considerations

To achieve the goal, perform the following configurations:

- Configure Device to work as the HTTPS server and request a certificate for Device.
- Request a certificate for Host so that Device can authenticate the identity of Host.
- Configure a CA server to issue certificates to Device and Host.

Configuration procedure

In this example, Windows Server works as the CA server and the Simple Certificate Enrollment Protocol (SCEP) plug-in is installed on the CA server.

Before performing the following configurations, make sure the switch, the host, and the CA server can reach each other.

1. Configure the HTTPS server (Device):

   # Create a PKI entity named **en**, and configure the common name as **http-server1** and the FQDN as **ssl.security.com**.

```
<Device> system-view
[Device] pki entity en
```

```
[Device-pki-entity-en] common-name http-server1
[Device-pki-entity-en] fqdn ssl.security.com
[Device-pki-entity-en] quit
```

# Create PKI domain **1**, specify the trusted CA as **ca server**, the URL of the registration server as **http://10.1.2.2/certsrv/mscep/mscep.dll**, the authority for certificate request as RA, and the entity for certificate request as **en**.

```
[Device] pki domain 1
[Device-pki-domain-1] ca identifier ca server
[Device-pki-domain-1] certificate request url
http://10.1.2.2/certsrv/mscep/mscep.dll
[Device-pki-domain-1] certificate request from ra
[Device-pki-domain-1] certificate request entity en
[Device-pki-domain-1] quit
```

# Create the local RSA key pairs.

```
[Device] public-key local create rsa
```

# Retrieve the CA certificate.

```
[Device] pki retrieval-certificate ca domain 1
```

# Request a local certificate for Device.

```
[Device] pki request-certificate domain 1
```

# Create an SSL server policy named **myssl**.

```
[Device] ssl server-policy myssl
```

# Specify the PKI domain for the SSL server policy as **1**.

```
[Device-ssl-server-policy-myssl] pki-domain 1
```

# Enable client authentication.

```
[Device-ssl-server-policy-myssl] client-verify enable
[Device-ssl-server-policy-myssl] quit
```

# Configure HTTPS service to use SSL server policy **myssl**.

```
[Device] ip https ssl-server-policy myssl
```

# Enable HTTPS service.

```
[Device] ip https enable
```

# Create a local user named **usera**, and set the password to **123** and service type to **web**.

```
[Device] local-user usera
[Device-luser-usera] password simple 123
[Device-luser-usera] service-type web
```

2. Configure the HTTPS client (Host):

   On Host, launch IE, enter http://10.1.2.2/certsrv in the address bar and request a certificate for Host as prompted.

3. Verify your configuration:

   Launch IE on the host, enter https://10.1.1.1 in the address bar, and select the certificate issued by the CA server. The web interface of the switch should appear. After entering username **usera** and password **123**, you should be able to log in to the web interface to access and manage the switch.

For more information about PKI configuration commands, see "Configuring PKI."

For more information about the **public-key local create rsa** command, see *Security Command Reference*.

For more information about HTTPS, see *Fundamentals Configuration Guide*.

Configuring an SSL client policy

An SSL client policy is a set of SSL parameters for a client to use when connecting to the server. An SSL client policy takes effect only after it is associated with an application layer protocol.

To configure an SSL client policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an SSL client policy and enter its view.	**ssl client-policy** *policy-name*	N/A
3. Specify a PKI domain for the SSL client policy.	**pki-domain** *domain-name*	Optional. No PKI domain is configured by default. After you specify a PKI domain, the SSL client requests a certificate through the PKI domain. If the SSL server requires certificate-based authentication for SSL clients, you must use this command to specify a PKI domain for the client. For more information about PKI domain configuration, see "Configuring PKI."

4. Specify the preferred cipher suite for the SSL client policy.	- In non-FIPS mode:
	prefer-cipher { **rsa_3des_ede_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:
	prefer-cipher { **dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_256_cbc_sha | rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** }
		Optional.
		rsa_rc4_128_md5 by default.

5. Specify the SSL protocol version for the SSL client policy.	- In non-FIPS mode: **version** { **ssl3.0** | **tls1.0** } - In FIPS mode: **version tls1.0**	Optional. TLS 1.0 by default.
6. Enable the SSL client to perform certificate-based authentication for the SSL server.	**server-verify enable**	Optional. Enabled by default.

Displaying and maintaining SSL

Task	Command	Remarks
Display SSL server policy information.	**display ssl server-policy** { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display SSL client policy information.	**display ssl client-policy** { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Troubleshooting SSL

Symptom

As the SSL server, the switch fails to handshake with the SSL client.

Analysis

SSL handshake failure may result from the following causes:

- The SSL client is configured to authenticate the SSL server, but the SSL server has no certificate or the certificate is not trusted.
- The SSL server is configured to authenticate the SSL client, but the SSL client has no certificate or the certificate is not trusted.
- The server and the client have no matching cipher suite.

Solution

1. Issue the **debugging ssl** command and view the debugging information to locate the problem:
   - If the SSL client is configured to authenticate the SSL server but the SSL server has no certificate, request one for it.
   - If the server's certificate cannot be trusted, install the root certificate of the CA that issued the local certificate to the SSL server on the SSL client, or let the server request a certificate from the CA that the SSL client trusts.
   - If the SSL server is configured to authenticate the client, but the SSL client has no certificate or the certificate cannot be trusted, request and install a certificate for the client.
2. Use the **display ssl server-policy** command to view the cipher suites that the SSL server policy supports. If the server and the client have no matching cipher suite, use the **ciphersuite** command to modify the cipher suite configuration of the SSL server.

Configuring TCP attack protection

Overview

An attacker can attack the switch during the process of establishing a TCP connection. To prevent such an attack, the switch provides the SYN Cookie feature.

Enabling the SYN Cookie feature

As a general rule, the establishment of a TCP connection involves the following three handshakes.

1. The request originator sends a SYN message to the target server.
2. After receiving the SYN message, the target server establishes a TCP connection in SYN_RECEIVED state, returns a SYN ACK message to the originator, and waits for a response.
3. After receiving the SYN ACK message, the originator returns an ACK message, establishing the TCP connection.

Attackers may mount SYN Flood attacks during TCP connection establishment. They send a large number of SYN messages to the server to establish TCP connections, but they never make any response to SYN ACK messages. As a result, a large number of incomplete TCP connections are established, resulting in heavy resource consumption and making the server unable to handle services normally.

The SYN Cookie feature can prevent SYN Flood attacks. After receiving a TCP connection request, the server directly returns a SYN ACK message, instead of establishing an incomplete TCP connection. Only after receiving an ACK message from the client can the server establish a connection, and then enter ESTABLISHED state. In this way, incomplete TCP connections could be avoided to protect the server against SYN Flood attacks.

Follow these guidelines when you enable the SYN Cookie feature:

With the SYN Cookie feature enabled, only the maximum segment size (MSS), is negotiated during TCP connection establishment, instead of the window's zoom factor and timestamp.

To enable the SYN Cookie feature:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the SYN Cookie feature.	**tcp syn-cookie enable**	Enabled by default

Displaying and maintaining TCP attack protection

Task	Command	Remarks
Display current TCP connection state.	**display tcp status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Configuring IP source guard

Overview

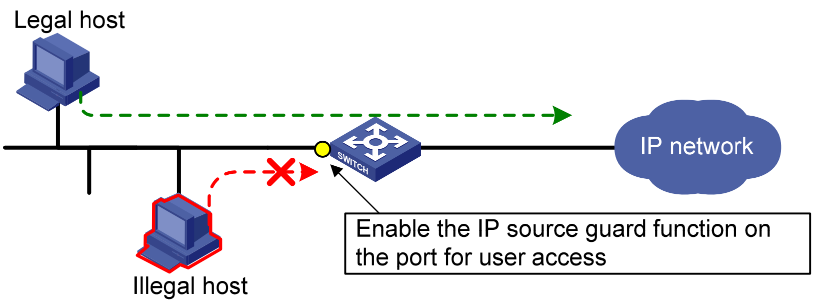
IP source guard is intended to improve port security by blocking illegal packets. For example, it can prevent illegal hosts from using a legal IP address to access the network.

IP source guard can filter packets according to the packet source IP address, source MAC address. IP source guard entries fall into the following types:

- IP-port binding entry
- MAC-port binding entry
- IP-MAC-port binding entry
- IP-VLAN-port binding entry
- MAC-VLAN-port binding entry
- IP-MAC-VLAN-port binding entry

After receiving a packet, an IP source guard-enabled port obtains the key attributes (source IP address, source MAC address and VLAN tag) of the packet and then looks them up in the IP source guard entries. If there is a match, the port forwards the packet. Otherwise, the port discards the packet, as shown in Figure 76.

Figure 76 Diagram for the IP source guard function


Legal host
IP network
SWITCH
Enable the IP source guard function on the port for user access
Illegal host

A binding entry can be statically configured or dynamically added.

Static IP source guard entries

A static IP source guard entry is configured manually. It is suitable for scenarios where few hosts exist on a LAN and their IP addresses are manually configured. For example, you can configure a static binding entry on a port that connects a server, allowing the port to receive packets from and send packets to only the server.

A static IPv4 source guard entry filters IPv4 packets received by the port or cooperates with ARP detection to check the validity of users. A static IPv6 source guard entry filters IPv6 packets received by the port cooperates with the ND detection feature to check the validity of users.

For information about ARP detection, see "Configuring ARP attack protection." For information about ND detection, see "Configuring ND attack defense."

A static IP source guard entry can be a global or port-based static binding entry.

Global static binding entry

A global static binding entry is a MAC-IP binding entry configured in system view. It is effective on all ports. A port forwards a packet when the packet's IP address and MAC address both match those of a global static binding entry or a static binding entry configured on the port.

Global static binding entries are used to protect against host spoofing attacks, which exploit the IP address or MAC address of a legal user host.

Port-based static binding entry

A port-based static binding entry binds an IP address, MAC address, or any combination of the two with a port. Such an entry is effective on only the specified port. A port forwards a packet only when the IP address, MAC address of the packet all match those in a static binding entry on the port or a global static binding entry. All other packets will be dropped.

Port-based static binding entries are used to check the validity of users who are trying to access a port.

Dynamic IP source guard entries

Dynamic IP source guard entries are generated dynamically according to client entries on the DHCP snooping or DHCP relay agent device. They are suitable for scenarios where many hosts reside on a LAN and obtain IP addresses through DHCP. Once DHCP allocates an IP address to a client, IP source guard automatically adds the client entry to allow the client to access the network. A user using an IP address not obtained through DHCP cannot access the network. Dynamic IPv6 source guard entries can also be obtained from client entries on the ND snooping device.

- Dynamic IPv4 source guard entries are generated dynamically based on DHCP snooping or DHCP relay entries to filter incoming IPv4 packets on a port.
- Dynamic IPv6 source guard entries are generated dynamically based on DHCPv6 snooping or ND snooping entries to filter incoming IPv6 packets on a port.

For information about DHCP snooping, DHCP relay, DHCPv6 snooping, and ND snooping, see *Layer 3—IP Services Configuration Guide*.

Configuration task list

Complete the following tasks to configure IPv4 source guard:

Task	Remarks
Configuring IPv4 source guard on a port	Required
Configuring a static IPv4 source guard entry	Optional
Setting the maximum number of IPv4 source guard entries	Optional

Complete the following tasks to configure IPv6 source guard:

Task	Remarks
Configuring IPv6 source guard on a port	Required
Configuring a static IPv6 source guard entry	Optional
Setting the maximum number of IPv6 source guard entries	Optional

Configuring the IPv4 source guard function

You cannot enable IPv4 source guard on a link aggregation member port. If IPv4 source guard is enabled on a port, you cannot assign the port to a link aggregation group.

Configuring IPv4 source guard on a port

The IPv4 source guard function must be configured on a port before the port can obtain dynamic IPv4 source guard entries and use static and dynamic IPv4 source guard entries to filter packets.

- For how to configure a static binding entry, see "Configuring a static IPv4 source guard entry."
- On a Layer 2 Ethernet port, IP source guard cooperates with DHCP snooping, dynamically obtains the DHCP snooping entries generated during dynamic IP address allocation, and generates IP source guard entries accordingly.
- On a VLAN interface, IP source guard cooperates with DHCP relay, dynamically obtains the DHCP relay entries generated during dynamic IP address allocation across network segments, and generates IP source guard entries accordingly.

Dynamic IPv4 source guard entries can contain such information as the MAC address, IP address, VLAN tag, ingress port information, and entry type (DHCP snooping or DHCP relay), where the MAC address, IP address, or VLAN tag information may not be included depending on your configuration. IP source guard applies these entries to the port to filter packets.

To generate IPv4 binding entries dynamically based on DHCP entries, make sure that DHCP snooping or DHCP relay is configured and working normally. For information about DHCP snooping configuration and DHCP relay configuration, see *Layer 3—IP Services Configuration Guide*.

If you repeatedly configure the IPv4 source guard function on a port, only the last configuration takes effect.

To configure the IPv4 source guard function on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	The term "interface" collectively refers to the following types of ports and interfaces: Bridge mode (Layer 2) Ethernet ports, VLAN interfaces, and port groups.
3. Configure IPv4 source guard on the port.	**ip verify source** { **ip-address** | **ip-address mac-address** | **mac-address** }	Not configured by default.

NOTE:

Although dynamic IPv4 source guard entries are generated based on DHCP entries, the number of dynamic IPv4 source guard entries is not necessarily the same as that of the DHCP entries.

Configuring a static IPv4 source guard entry

Static IPv4 binding entries take effect only on the ports configured with the IPv4 source guard function (see "Configuring IPv4 source guard on a port").

Port-based static IPv4 source guard entries and dynamic IPv4 source guard entries take precedence over global static IPv4 source guard entries. A port matches a packet against global static binding entries only when the packet does not match any port-based static binding entry or dynamic binding entry on the port.

Configuring global static IPv4 binding entries

A global static binding entry defines the IP address and MAC address of the packets that can be forwarded by ports. It takes effect on all ports of the device.

To configure a global static IPv4 binding entry:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a global static IPv4 binding entry.	**ip source binding ip-address** *ip-address* **mac-address** *mac-address*	No global static IPv4 binding entry is configured by default.

Configuring port-based static IPv4 binding entries

Follow these guidelines to configure port-based static IPv4 source guard entries:

- You cannot repeatedly configure the same static binding entry on one port, but you can configure the same static entry on different ports.
- IP source guard does not use the VLAN information (if specified) in static IPv4 binding entries to filter packets.
- When the ARP detection function is configured, be sure to specify the VLAN where ARP detection is configured in static IPv4 binding entries. Otherwise, ARP packets are discarded because they cannot match any static IPv4 binding entry.
- If a static binding entry to be added denotes the same binding as an existing dynamic binding entry, the new static binding entry overwrites the dynamic binding entry.

To configure a static IPv4 binding entry on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 interface view.	**interface** *interface-type interface-number*	N/A
3. Configure a static IPv4 source guard entry on the port.	**ip source binding** { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	By default, no static IPv4 binding entry is configured on a port.

Setting the maximum number of IPv4 source guard entries

The maximum number of IPv4 source guard entries is used to limit the total number of static and dynamic IPv4 source guard entries on a port. When the number of IPv4 binding entries on a port reaches the maximum, the port does not allowed new IPv4 binding entries any more.

If the maximum number of IPv4 binding entries to be configured is smaller than the number of existing IPv4 binding entries on the port, the maximum number can be configured successfully, and the existing entries are not affected. New IPv4 binding entries, however, cannot be added until the number of IPv4 binding entries on the port drops below the configured maximum.

To configure the maximum number of IPv4 binding entries allowed on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the maximum number of IPv4 binding entries allowed on the port.	**ip verify source max-entries** *number*	Optional. 640 by default.

Configuring the IPv6 source guard function

You cannot enable IPv6 source guard on a link aggregation member port or a service loopback port. If IPv6 source guard is enabled on a port, you cannot assign the port to a link aggregation group.

Configuring IPv6 source guard on a port

The IPv6 source guard function must be configured on a port before the port can obtain dynamic IPv6 source guard entries and use static and dynamic IPv6 source guard entries to filter packets.

- For how to configure a static IPv6 static binding entry, see "Configuring a static IPv6 source guard entry."
- Cooperating with DHCPv6 snooping, IP source guard dynamically generates IP source guard entries based on the DHCPv6 snooping entries that are generated during dynamic IP address allocation.
- Cooperating with ND snooping, IP source guard dynamically generates IP source guard entries based on dynamic ND snooping entries.

Dynamic IPv6 source guard entries can contain such information as the MAC address, IPv6 address, VLAN tag, ingress port information and entry type (DHCPv6 snooping or ND snooping), where the MAC address, IPv6 address, and/or VLAN tag information may not be included depending on your configuration. IP source guard applies these entries to the port, so that the port can filter packets accordingly.

Follow these guidelines when you configure IPv6 source guard:

- If you repeatedly configure the IPv6 source guard function, only the last configuration takes effect.
- To obtain dynamic IPv6 source guard entries, make sure that DHCPv6 snooping or ND snooping is configured and works normally. For DHCPv6 and ND snooping configuration information, see *Layer 3—IP Services Configuration Guide*.

- If you configure both ND snooping and DHCPv6 snooping on the device, IPv6 source guard uses the type of entries that generated first. Because DHCPv6 snooping entries are usually generated first in such a case, IPv6 source guard usually uses the DHCPv6 snooping entries to filter packets on a port.

To configure the IPv6 source guard function on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view, or port group view.	**interface** *interface-type interface-number*	N/A
3. Configure the IPv6 source guard function on the port.	**ipv6 verify source** { **ipv6-address** | **ipv6-address mac-address** | **mac-address** }	Not configured by default. The keyword specified in the **ipv6 verify source** command is only for instructing the generation of dynamic IPv6 source guard entries. It does not affect static binding entries. When using a static binding entry, a port does not consider the keyword into consideration.

NOTE:

Although dynamic IPv6 source guard entries are generated based on DHCPv6 entries, the number of dynamic IPv6 source guard entries is not necessarily the same as that of the DHCPv6 entries.

Configuring a static IPv6 source guard entry

Static IPv6 binding entries take effect only on ports configured with the IPv6 source guard function (see "Configuring the IPv6 source guard function").

Port-based static IPv6 source guard entries and dynamic IPv6 source guard entries take precedence over global static IPv6 source guard entries. A port matches a packet against global static binding entries only when the packet does not match any port-based static binding entry or dynamic binding entry on the port.

Configuring global static IPv6 binding entries

A global static IPv6 binding entry defines the IPv6 address and MAC address of the packets that can be forwarded by ports. It takes effect on all ports of the device.

To configure a global static IPv6 binding entry:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a global static IPv6 binding entry.	**ipv6 source binding ipv6-address** *ipv6-address* **mac-address** *mac-address*	No global static IPv6 binding entry is configured by default.

Configuring port-based static IPv6 binding entries

Follow these guidelines to configure port-based static IPv6 source guard entries:

- You cannot configure the same static binding entry on one port repeatedly, but you can configure the same static binding entry on different ports.
- In an IPv6 source guard entry, the MAC address cannot be all 0s, all Fs (a broadcast MAC address), or a multicast address, and the IPv6 address must be a unicast address and cannot be all 0s, all Fs, or a loopback address.
- IP source guard does not use the VLAN information (if specified) in static IPv6 binding entries to filter packets.
- When the ND detection function is configured, be sure to specify the VLAN where ND detection is configured in static binding entries. Otherwise, ND packets will be discarded because they cannot match any static IPv6 binding entry.
- If a static binding entry to be added denotes the same binding as an existing dynamic binding entry, the new static binding entry overwrites the dynamic binding entry.

To configure a static IPv6 source guard entry on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 interface view.	**interface** *interface-type interface-number*	N/A
3. Configure a static IPv6 binding entry on a port.	**ipv6 source binding** { **ipv6-address** *ipv6-address* | **ipv6-address** *ipv6-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]	By default, no static IPv6 binding entry is configured on a port.

Setting the maximum number of IPv6 source guard entries

The maximum number of IPv6 source guard entries is used to limit the total number of static and dynamic IPv6 source guard entries on a port. When the number of IPv6 binding entries on a port reaches the maximum, the port does not allow new IPv6 binding entries any more.

If the maximum number of IPv6 binding entries to be configured is smaller than the number of existing IPv6 binding entries on the port, the maximum number can be configured successfully, and the existing entries are not affected. New IPv6 binding entries, however, cannot be added until the number of IPv6 binding entries on the port drops below the configured maximum.

To configure the maximum number of IPv6 binding entries allowed on a port:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the maximum number of IPv6 binding entries allowed on the port.	**ipv6 verify source max-entries** *number*	Optional. 640 by default.

Displaying and maintaining IP source guard

For IPv4 source guard:

Task	Command	Remarks
Display static IPv4 source guard entries.	**display ip source binding static** [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display IPv4 source guard entries.	**display ip source binding** [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

For IPv6 source guard:

Task	Command	Remarks
Display static IPv6 source guard entries.	**display ipv6 source binding static** [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display IPv6 source guard entries.	**display ipv6 source binding** [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address*] [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

IP source guard configuration examples

Static IPv4 source guard configuration example

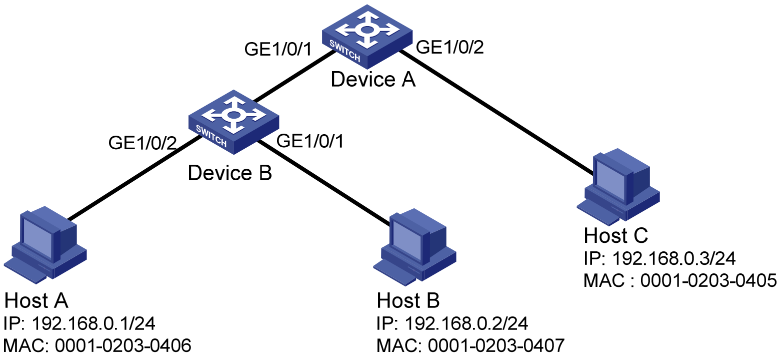
Network requirements

As shown in Figure 77, Host A and Host B are connected to ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/1 of Device B respectively, Host C is connected to port GigabitEthernet 1/0/2 of Device A, and Device B is connected to port GigabitEthernet 1/0/1 of Device A. All hosts use static IP addresses.

Configure static IPv4 source guard entries on Device A and Device B to meet the following requirements:

- On port GigabitEthernet 1/0/2 of Device A, only IP packets from Host C can pass.
- On port GigabitEthernet 1/0/1 of Device A, only IP packets from Host A can pass.
- On port GigabitEthernet 1/0/2 of Device B, only IP packets from Host A can pass.
- On port GigabitEthernet 1/0/1 of Device B, only IP packets sourced from 192.168.0.2/24 can pass. Host B can communicate with Host A by using this IP address even if it uses another network adapter.

Figure 77 Network diagram



Configuration procedure

1. Configure Device A:

   # Configure the IPv4 source guard function on GigabitEthernet 1/0/2 to filter packets based on both the source IP address and MAC address.

   ```
   <DeviceA> system-view
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
   ```

   # Configure GigabitEthernet 1/0/2 to allow only IP packets with the source MAC address of 0001-0203-0405 and the source IP address of 192.168.0.3 to pass.

   ```
   [DeviceA] interface gigabitethernet 1/0/2
   [DeviceA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address
   0001-0203-0405
   [DeviceA-GigabitEthernet1/0/2] quit
   ```

   # Configure the IPv4 source guard function on GigabitEthernet 1/0/1 to filter packets based on both the source IP address and MAC address.

   ```
   [DeviceA] interface gigabitethernet 1/0/1
   [DeviceA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
   ```

   # Configure GigabitEthernet 1/0/1 to allow only IP packets with the source MAC address of 0001-0203-0406 and the source IP address of 192.168.0.1 to pass.

   ```
   [DeviceA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
   0001-0203-0406
   [DeviceA-GigabitEthernet1/0/1] quit
   ```

2. Configure Device B:

   # Configure the IPv4 source guard function on GigabitEthernet 1/0/2 to filter packets based on both the source IP address and MAC address.

   ```
   <DeviceB> system-view
   [DeviceB] interface gigabitethernet 1/0/2
   [DeviceB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
   ```

   # Configure GigabitEthernet 1/0/2 to allow only IP packets with the source MAC address of 0001-0203-0406 and the source IP address of 192.168.0.1 to pass.

   ```
   [DeviceB] interface gigabitethernet 1/0/2
   [DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.1 mac-address
   0001-0203-0406
   [DeviceB-GigabitEthernet1/0/2] quit
   ```

# Configure the IPv4 source guard function on GigabitEthernet 1/0/1 to filter packets based on the source IP address.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip verify source ip-address
```

# Configure GigabitEthernet 1/0/1 to allow only IP packets with the source IP address of 192.168.0.2 to pass.

```
[DeviceB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2
[DeviceB-GigabitEthernet1/0/1] quit
```

Verifying the configuration

# On Device A, display information about static IPv4 source guard entries. The output shows that the static IPv4 source guard entries are configured successfully.

```
[DeviceA] display ip source binding static
Total entries found: 2
 MAC Address         IP Address        VLAN    Interface                Type
 0001-0203-0405      192.168.0.3       N/A     GE1/0/2                  Static
 0001-0203-0406      192.168.0.1       N/A     GE1/0/1                  Static
```

# On Device B, display information about static IPv4 source guard entries. The output shows that the static IPv4 source guard entries are configured successfully.

```
[DeviceB] display ip source binding static
Total entries found: 2
 MAC Address         IP Address        VLAN    Interface                Type
 0001-0203-0406      192.168.0.1       N/A     GE1/0/2                  Static
 N/A                 192.168.0.2       N/A     GE1/0/1                  Static
```

Dynamic IPv4 source guard using DHCP snooping configuration example

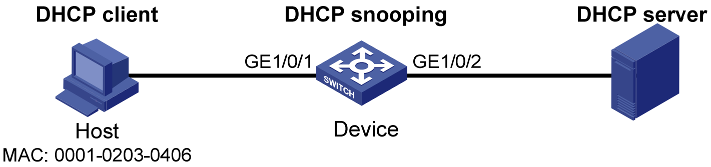
Network requirements

As shown in Figure 78, the device connects to the host (client) and the DHCP server through ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 respectively. The host obtains an IP address from the DHCP server.

Enable DHCP snooping on the device to record the DHCP snooping entry of the host. Enable the IPv4 source guard function on the device's port GigabitEthernet 1/0/1 to filter packets based on the DHCP snooping entry, allowing only packets from clients that obtain IP addresses through the DHCP server to pass.

For information about DHCP server configuration, see *Layer 3—IP Services Configuration Guide*.

Figure 78 Network diagram



Configuration procedure

1. Configure DHCP snooping.

# Enable DHCP snooping.

```
<Device> system-view
[Device] dhcp-snooping
```

# Configure port GigabitEthernet 1/0/2, which is connected to the DHCP server, as a trusted port.

```
[Device] interface gigabitethernet1/0/2
[Device-GigabitEthernet1/0/2] dhcp-snooping trust
[Device-GigabitEthernet1/0/2] quit
```

2. Configure the IPv4 source guard function.

   # Configure the IPv4 source guard function on port GigabitEthernet 1/0/1 to filter packets based on both the source IP address and MAC address.

```
[Device] interface gigabitethernet1/0/1
[Device-GigabitEthernet1/0/1] ip verify source ip-address mac-address
[Device-GigabitEthernet1/0/1] quit
```

Verifying the configuration

# Display the IPv4 source guard entries generated on port GigabitEthernet 1/0/1.

```
[Device] display ip source binding
Total entries found: 1
 MAC Address        IP Address       VLAN    Interface            Type
 0001-0203-0406     192.168.0.1      1       GE1/0/1              DHCP-SNP
```

# Display DHCP snooping entries to see whether they are consistent with the dynamic entries generated on GigabitEthernet 1/0/1.

```
[Device] display dhcp-snooping
 DHCP snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static , R--Recovering
 Type IP Address      MAC Address    Lease        VLAN SVLAN Interface
 ==== =============== ============== ============ ==== ===== =================
 D    192.168.0.1     0001-0203-0406 86335        1    N/A   GigabitEthernet1/0/1
---    1 dhcp-snooping item(s) found   ---
```

The output shows that a dynamic IPv4 source guard entry has been generated based on the DHCP snooping entry.

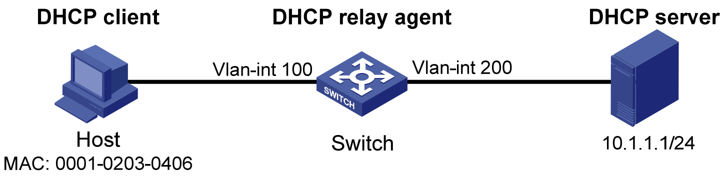
Dynamic IPv4 source guard using DHCP relay configuration example

Network requirements

As shown in Figure 79, the host and the DHCP server are connected to the switch through interfaces VLAN-interface 100 and VLAN-interface 200 respectively. DHCP relay is enabled on the switch. The host (with the MAC address of 0001-0203-0406) obtains an IP address from the DHCP server through the DHCP relay agent.

Enable the IPv4 source guard function on the switch's VLAN-interface 100 to filter packets based on the DHCP relay entry, allowing only packets from clients that obtain IP addresses from the DHCP server to pass.

Figure 79 Network diagram



Configuration procedure

1. Configure the IPv4 source guard function:

   # Configure the IP addresses of the interfaces. (Details not shown.)

   # Configure the IPv4 source guard function on VLAN-interface 100 to filter packets based on both the source IP address and MAC address.

```
<Switch> system-view
[Switch] vlan 100
[Switch-Vlan100] quit
[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
```

   # Configure the IP address of the DHCP server.

```
[Switch] dhcp relay server-group 1 ip 10.1.1.1
```

   # Configure VLAN-interface 100 to operate in DHCP relay mode.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] dhcp select relay
```

   # Correlate VLAN-interface 100 with DHCP server group 1.

```
[Switch-Vlan-interface100] dhcp relay server-select 1
[Switch-Vlan-interface100] quit
```

Verifying the configuration

# Display the generated IPv4 source guard entries.

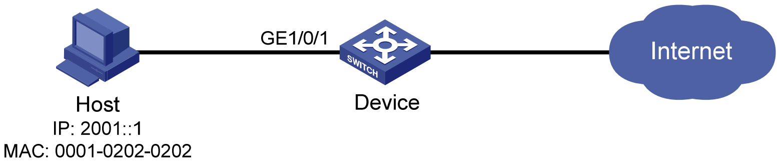
```
[Switch] display ip source binding
Total entries found: 1
 MAC Address        IP Address      VLAN    Interface               Type
 0001-0203-0406     192.168.0.1     100     Vlan100                 DHCP-RLY
```

Static IPv6 source guard configuration example

Network requirements

As shown in Figure 80, the host is connected to port GigabitEthernet 1/0/1 of the device. Configure a static IPv6 source guard entry for GigabitEthernet 1/0/1 of the device to allow only packets from the host to pass.

Figure 80 Network diagram



Configuration procedure

# Configure the IPv6 source guard function on GigabitEthernet 1/0/1 to filter packets based on both the source IP address and MAC address.

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
```

# Configure GigabitEthernet 1/0/1 to allow only IPv6 packets with the source MAC address of 0001-0202-0202 and the source IPv6 address of 2001::1 to pass.

```
[Device-GigabitEthernet1/0/1] ipv6 source binding ipv6-address 2001::1 mac-address
0001-0202-0202
[Device-GigabitEthernet1/0/1] quit
```

Verifying the configuration

# On Device, display the information about static IPv6 source guard entries. The output shows that the binding entry is configured successfully.

```
[Device] display ipv6 source binding static
Total entries found: 1
 MAC Address        IP Address        VLAN   Interface               Type
 0001-0202-0202     2001::1           N/A    GE1/0/1                 Static-IPv6
```

Dynamic IPv6 source guard using DHCPv6 snooping configuration example

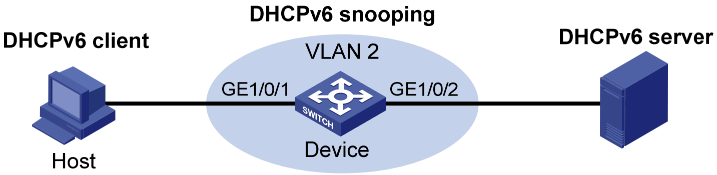
Network requirements

As shown in Figure 81, the host (DHCPv6 client) and the DHCPv6 server are connected to the device through ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 respectively.

Enable DHCPv6 and DHCPv6 snooping on the device, so that the host can obtain an IP address through the DHCPv6 server and the IPv6 IP address and the MAC address of the host can be recorded in a DHCPv6 snooping entry.

Enable IPv6 source guard function on the device's port GigabitEthernet 1/0/1 to filter packets based on DHCPv6 snooping entries, allowing only packets from a client that obtains an IP address through the DHCP server to pass.

Figure 81 Network diagram



Configuration procedure

1. Configure DHCPv6 snooping:

   # Enable DHCPv6 snooping globally.

   ```
   <Device> system-view
   [Device] ipv6 dhcp snooping enable
   ```

   # Enable DHCPv6 snooping in VLAN 2.

   ```
   [Device] vlan 2
   [Device-vlan2] ipv6 dhcp snooping vlan enable
   [Device-vlan2] quit
   ```

   # Configure the port connecting to the DHCP server as a trusted port.

   ```
   [Device] interface gigabitethernet 1/0/2
   [Device-GigabitEthernet1/0/2] ipv6 dhcp snooping trust
   [Device-GigabitEthernet1/0/2] quit
   ```

2. Configure the IPv6 source guard function:

   # Configure the IPv6 source guard function on GigabitEthernet 1/0/1 to filter packets based on both the source IP address and MAC address.

   ```
   [Device] interface gigabitethernet 1/0/1
   [Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
   [Device-GigabitEthernet1/0/1] quit
   ```

Verifying the configuration

# Display the dynamic IPv6 source guard entries generated on port GigabitEthernet 1/0/1.

```
[Device] display ipv6 source binding
Total entries found: 1
 MAC Address          IP Address         VLAN   Interface        Type
 040a-0000-0001       2001::1            2      GE1/0/1          DHCPv6-SNP
```

# Display all DHCPv6 snooping entries to see whether they are consistent with the dynamic IP source guard entries generated on GigabitEthernet 1/0/1.

```
[Device] display ipv6 dhcp snooping user-binding dynamic
IP Address                     MAC Address    Lease      VLAN Interface
============================== ============== ========== ==== ==================
2001::1                        040a-0000-0001 286        2    GigabitEthernet1/0/1
---   1 DHCPv6 snooping item(s) found   ---
```

The output shows that a dynamic IPv6 source guard entry has been generated on port GigabitEthernet 1/0/1 based on the DHCPv6 snooping entry.

Dynamic IPv6 source guard using ND snooping configuration example

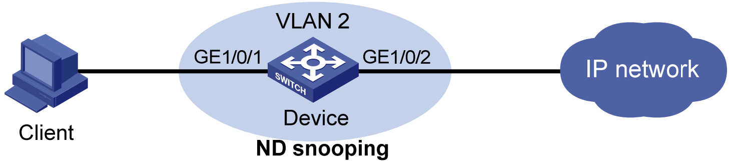
Network requirements

As shown in Figure 82, the client is connected to the device through port GigabitEthernet 1/0/1.

Enable ND snooping on the device, establishing ND snooping entries by listening to DAD NS messages.

Enable the IPv6 source guard function on port GigabitEthernet 1/0/1 to filter packets based on the ND snooping entries, allowing only packets with a legally obtained IPv6 address to pass.

Figure 82 Network diagram



Configuration procedure

1. Configure ND snooping:

   # In VLAN 2, enable ND snooping.

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] ipv6 nd snooping enable
[Device-vlan2] quit
```

2. Configure the IPv6 source guard function:

   # Configure the IPv6 source guard function on GigabitEthernet 1/0/1 to filter packets based on both the source IP address and MAC address.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
[Device-GigabitEthernet1/0/1] quit
```

Verifying the configuration

# Display the IPv6 source guard entries generated on port GigabitEthernet 1/0/1.

```
[Device] display ipv6 source binding
Total entries found: 1
 MAC Address          IP Address         VLAN   Interface       Type
 040a-0000-0001       2001::1            2      GE1/0/1         ND-SNP
```

# Display the IPv6 ND snooping entries to see whether they are consistent with the dynamic IP source guard entries generated on GigabitEthernet 1/0/1.

```
[Device] display ipv6 nd snooping
IPv6 Address                  MAC Address     VID  Interface      Aging Status
2001::1                       040a-0000-0001  2    GE1/0/1        25     Bound
---- Total entries: 1 ----
```

The output shows that a dynamic IPv6 source guard entry has generated on port GigabitEthernet 1/0/1 based on the ND snooping entry.

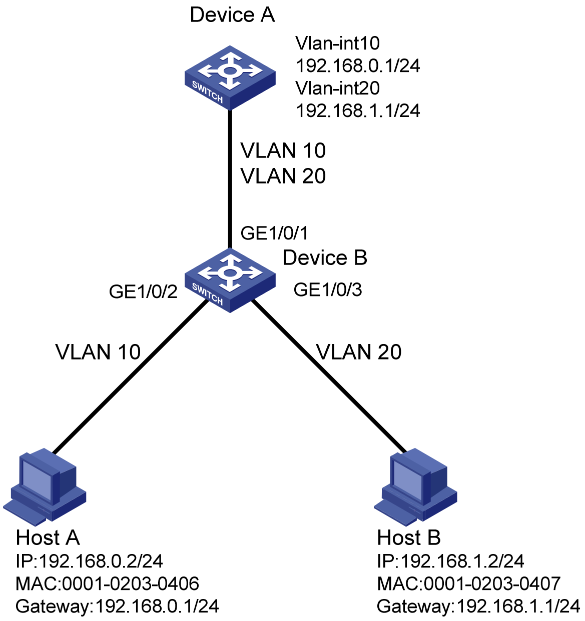
Global static IP source guard configuration example

Network requirements

As shown in Figure 83, Device A is a distribution layer device. Device B is an access device. Host A in VLAN 10 and Host B in VLAN 20 communicate with each other through Device A.

- Configure Device B to discard attack packets that exploit the IP address or MAC address of Host A and Host B.
- Configure Device B to forward packets of Host A and Host B normally.

Figure 83 Network diagram



Configuration procedure

# Create VLAN 10, and add port GigabitEthernet 1/0/2 to VLAN 10.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] port gigabitethernet 1/0/2
[DeviceB-vlan10] quit
```

# Create VLAN 20, and add port GigabitEthernet 1/0/3 to VLAN 20.

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/3
[DeviceB-vlan20] quit
```

# Configure the link type of GigabitEthernet 1/0/1 as trunk, and permit packets of VLAN 10 and VLAN 20 to pass the port.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[DeviceB-GigabitEthernet1/0/1] quit
```

# Configure IPv4 source guard on GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 to filter packets based on both the source IP address and MAC address.

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet1/0/3] quit
```

# Configure global static IP binding entries to prevent attack packets that exploit the IP address or MAC address of Host A and Host B from being forwarded.

```
[DeviceB] ip source binding ip-address 192.168.0.2 mac-address 0001-0203-0406
```

```
[DeviceB] ip source binding ip-address 192.168.1.2 mac-address 0001-0203-0407
```

Verifying the configuration

# Display static IPv4 binding entries on Device B.

```
[DeviceB] display ip source binding static
Total entries found: 2
 MAC Address        IP Address       VLAN   Interface             Type
 0001-0203-0406     192.168.0.2      N/A    N/A                   Static
 0001-0203-0407     192.168.1.2      N/A    N/A                   Static
```

After the configurations, Host A and Host B can ping each other successfully.

Troubleshooting IP source guard

Symptom

Failed to configure static or dynamic IP source guard on a port.

Analysis

IP source guard is not supported on a port in an aggregation group.

Solution

Remove the port from the aggregation group.

Configuring ARP attack protection

Overview

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 destination unreachable IP packets to have the receiving device busy with resolving destination IP addresses until its CPU is overloaded.
- 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 attacks and viruses are threatening LAN security. This chapter introduces multiple features to detect and prevent such attacks.

ARP attack protection configuration task list

Task			Remarks
Flood prevention	Configuring ARP defense against IP packet attacks	Configuring ARP source suppression	Optional. Configure this function on gateways (recommended).
		Enabling ARP black hole routing	Optional. Configure this function on gateways (recommended).
	Configuring ARP packet rate limit		Optional. Configure this function on access devices (recommended).
	Configuring source MAC address based ARP attack detection		Optional. Configure this function on gateways (recommended).
User and gateway spoofing prevention	Configuring ARP packet source MAC address consistency check		Optional. Configure this function on gateways (recommended).
	Configuring ARP active acknowledgement		Optional. Configure this function on gateways (recommended).
	Configuring ARP detection		Optional. Configure this function on access devices (recommended).

Task		Remarks
	Configuring ARP automatic scanning and fixed ARP	Optional. Configure this function on gateways (recommended).
	Configuring ARP gateway protection	Optional. Configure this function on access devices (recommended).
	Configuring ARP filtering	Optional. Configure this function on access devices (recommended).

Configuring ARP defense against IP packet attacks

If the device receives a large number of IP packets from a host addressed to unreachable destinations:

- The device sends a large number of ARP requests to the destination subnets, and thus the load of the destination subnets increases.
- The device keeps trying to resolve destination IP addresses, which increases the load on the CPU.

To protect the device from IP packet attacks, you can enable the ARP source suppression function or ARP black hole routing function.

If the packets have the same source address, you can enable the ARP source suppression function. With the function enabled, you can set a threshold for the number of ARP requests that a sending host can trigger in 5 seconds with packets with unresolvable destination IP addresses. When the number of ARP requests exceeds that threshold, the device suppresses the host from triggering any ARP requests in the following 5 seconds.

If the packets have various source addresses, you can enable the ARP black hole routing function. After receiving an IP packet whose destination IP address cannot be resolved by ARP, the device with this function enabled immediately creates a black hole route and simply drops all packets matching the route during the aging time of the black hole route.

Configuring ARP source suppression

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable ARP source suppression.	**arp source-suppression enable**	Disabled by default.
3.	Set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in 5 consecutive seconds.	**arp source-suppression limit** *limit-value*	Optional. 10 by default.

Enabling ARP black hole routing

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable ARP black hole routing.	**arp resolving-route enable**	Optional. Enabled by default.

Displaying and maintaining ARP defense against IP packet attacks

Task	Command	Remarks
Display ARP source suppression configuration information.	**display arp source-suppression** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

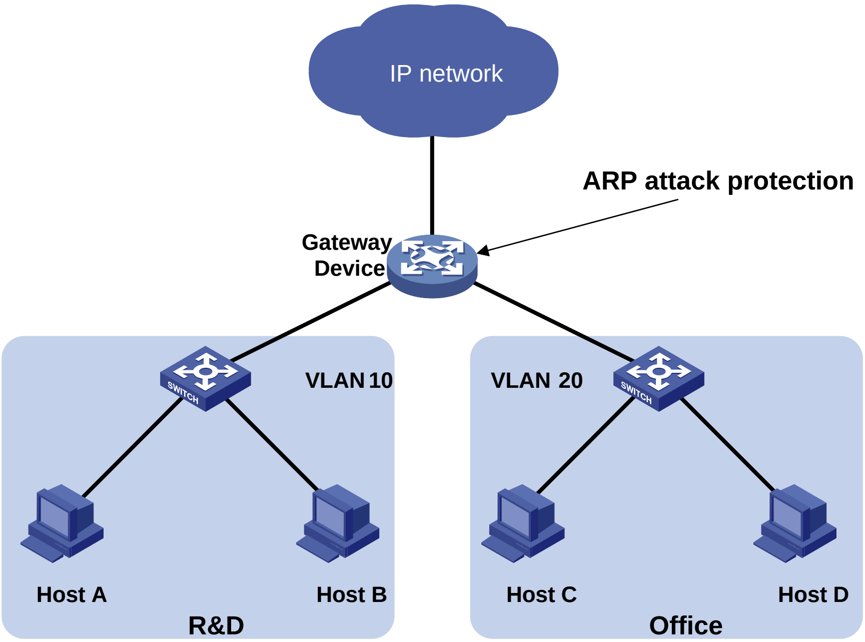
Configuration example

Network requirements

As shown in Figure 84, a LAN contains two areas: an R&D area in VLAN 10 and an office area in VLAN 20. The two areas connect 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 IP flood attack. To prevent such attacks, configure ARP source suppression and ARP black hole routing.

Figure 84 Network diagram



Configuration considerations

If the attacking packets have the same source address, you can enable the ARP source suppression function with the following steps:

1. Enable ARP source suppression.
2. Set the threshold for ARP packets from the same source address to 100. If the number of ARP requests sourced from the same IP address in 5 seconds exceeds 100, the device suppresses the IP packets sourced from this IP address from triggering any ARP requests within the following 5 seconds.

If the attacking packets have different source addresses, enable the ARP black hole routing function on the device.

Configuration procedure

1. Enable ARP source suppression on the device and set the threshold for ARP packets from the same source address to 100.

```
<Device> system-view
[Device] arp source-suppression enable
[Device] arp source-suppression limit 100
```

2. Enable ARP black hole routing on the device.

```
<Device> system-view
[Device] arp resolving-route enable
```

Configuring ARP packet rate limit

Introduction

The ARP packet rate limit feature allows you to limit the rate of ARP packets to be delivered to the CPU on a switch. For example, if an attacker sends a large number of ARP packets to an ARP detection enabled device, the CPU of the device will be overloaded because all of the ARP packets are redirected to the CPU for checking. As a result, the device fails to deliver other functions properly or even crashes. To solve this problem, you can configure ARP packet rate limit.

Enable this feature after the ARP detection, or ARP snooping feature is configured, or use this feature to prevent ARP flood attacks.

Configuration procedure

When the ARP packet rate exceeds the rate limit set on an interface, the device with ARP packet rate limit enabled sends trap and log messages to inform the event. To avoid too many trap and log messages, you can set the interval for sending such messages. Within each interval, the device will output the peak ARP packet rate in the trap and log messages.

Note that trap and log messages are generated only after the trap function of ARP packet rate limit is enabled. Trap and log messages will be sent to the information center of the device. You can set the parameters of the information center to determine the output rules of trap and log messages. The output rules specify whether the messages are allowed to be output and where they are bound for. For the parameter configuration of the information center, see *Network Management and Monitoring Configuration Guide*.

If you enable ARP packet rate limit on a Layer 2 aggregate interface, trap and log messages are sent when the ARP packet rate of a member port exceeds the preset threshold rate.

To configure ARP packet rate limit:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable ARP packet rate limit trap.	**snmp-agent trap enable arp rate-limit**	Optional. Enabled by default. For more information, see the **snmp-agent trap enable arp** command in *Network Management and Monitoring Command Reference*.
3. Set the interval for sending trap and log messages when ARP packet rate exceeds the specified threshold rate.	**arp rate-limit information interval** *seconds*	Optional. 60 seconds by default.
4. Enter Layer 2 Ethernet interface/Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
5. Configure ARP packet rate limit.	**arp rate-limit** { **disable** | **rate** *pps* **drop** }	By default, ARP packet rate limit is disabled.

Configuring source MAC address based ARP attack detection

With this feature enabled, the device checks the source MAC address of ARP packets delivered to the CPU. It detects an attack when one MAC address sends more ARP packets in 5 seconds than the specified threshold. The device adds the MAC address to the attack detection table.

Before the attack detection entry is aged out, the device uses either of the following detection modes to respond to the detected attack:

- **Monitor mode**—Generates a log message.
- **Filter mode**—Generates a log message and filters out subsequent ARP packets from the attacking MAC address.

You can also configure protected MAC addresses to exclude a gateway or server from detection. A protected MAC address is excluded from ARP attack detection even if it is an attacker.

Configuration procedure

To configure source MAC address based ARP attack detection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enable source MAC address based ARP attack detection and specify the detection mode.	**arp anti-attack source-mac** { **filter** | **monitor** }	Disabled by default.
3. Configure the threshold.	**arp anti-attack source-mac threshold** *threshold-value*	Optional. 50 by default.
4. Configure the age timer for ARP attack detection entries.	**arp anti-attack source-mac aging-time** *time*	Optional. 300 seconds by default.
5. Configure protected MAC addresses.	**arp anti-attack source-mac exclude-mac** *mac-address*&<1-10>	Optional. Not configured by default.

NOTE:

After an ARP attack detection entry expires, ARP packets sourced from the MAC address in the entry can be processed normally.

Displaying and maintaining source MAC address based ARP attack detection

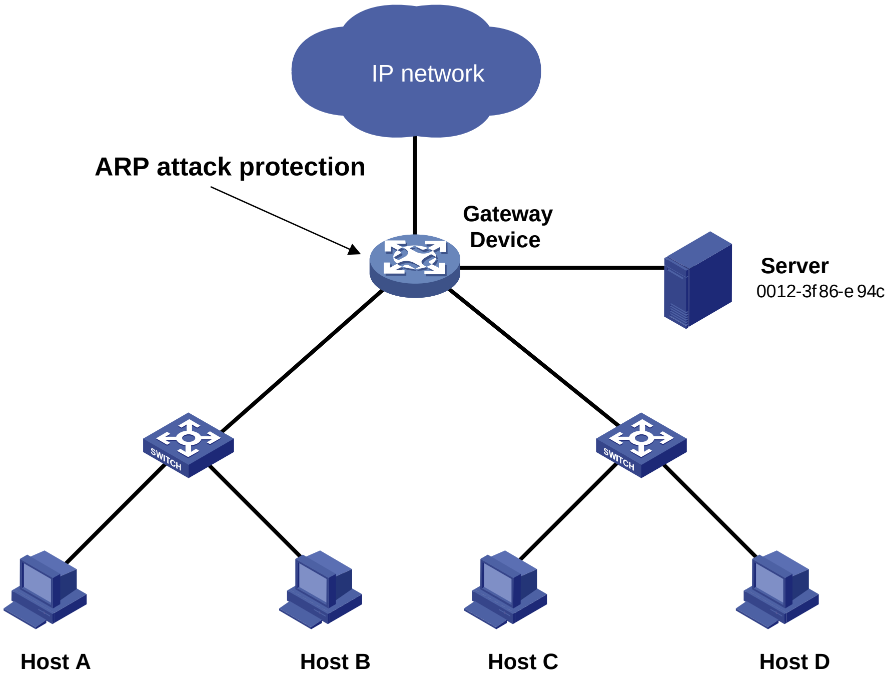
Task	Command	Remarks
Display attacking MAC addresses detected by source MAC address based ARP attack detection.	**display arp anti-attack source-mac** { **slot** *slot-number* | **interface** *interface-type interface-number* } [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Configuration example

Network requirements

As shown in Figure 85, the hosts access the Internet through a gateway (Device). If malicious users send a large number of ARP requests to the gateway, the gateway may crash and cannot process requests from the clients. To solve this problem, configure source MAC address based ARP attack detection on the gateway.

Figure 85 Network diagram



Configuration considerations

An attacker may 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 address based ARP attack detection and specify the filter mode.
2. Set the threshold.
3. Set the age timer for detection entries.
4. Configure the MAC address of the server as a protected MAC address so that it can send ARP packets

Configuration procedure

# Enable source MAC address based ARP attack detection and specify the filter mode.

```
<Device> system-view
[Device] arp anti-attack source-mac filter
```

# Set the threshold to 30.

```
[Device] arp anti-attack source-mac threshold 30
```

# Set the age timer for detection entries to 60 seconds.

```
[Device] arp anti-attack source-mac aging-time 60
```

# Configure 0012-3f86-e94c as a protected MAC address.

```
[Device] arp anti-attack source-mac exclude-mac 0012-3f86-e94c
```

Configuring ARP packet source MAC address consistency check

Introduction

The ARP packet source MAC address consistency check feature enables a gateway device to filter out ARP packets that have a different source MAC address in the Ethernet header from the sender MAC address in the message, so that the gateway device can learn correct ARP entries.

Configuration procedure

To enable ARP packet source MAC address consistency check:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable ARP packet source MAC address consistency check.	**arp anti-attack valid-check enable**	Disabled by default

Configuring ARP active acknowledgement

Introduction

The ARP active acknowledgement feature is configured on gateway devices to identify invalid ARP packets.

ARP active acknowledgement works before the gateway creates or modifies an ARP entry to avoid generating any incorrect ARP entry. For more information about its working mechanism, see *ARP Attack Protection Technology White Paper*.

Configuration procedure

To configure ARP active acknowledgement:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the ARP active acknowledgement function.	**arp anti-attack active-ack enable**	Disabled by default

Configuring ARP detection

Introduction

ARP detection enables access devices to block ARP packets from unauthorized clients to prevent user spoofing and gateway spoofing attacks.

ARP detection provides the user validity check, ARP packet validity check, and ARP restricted forwarding functions. If both ARP packet validity check and user validity check are enabled, the former one applies first, and then the latter applies.

ARP detection does not check ARP packets received from ARP trusted ports.

Configuring user validity check

This feature enables a device to check user validity as follows:

1. Upon receiving an ARP packet from an ARP untrusted interface, the device checks the packet against the configured rules. If a match is found, the ARP packet is processed according to the matching rule. If no match is found, the device checks the packet against static IP Source Guard binding entries
2. The device compares the sender IP and MAC addresses of the ARP packet against the static IP source guard binding entries. If a match is found, the ARP packet is considered valid and is forwarded. If an entry with a matching IP address but an unmatched MAC address is found, the ARP packet is considered invalid and is discarded. If no entry with a matching IP address is found, the device compares the ARP packet's sender IP and MAC addresses against the DHCP snooping entries, 802.1X security entries, and OUI MAC addresses.
3. If a match is found from those entries, the ARP packet is considered valid and is forwarded. (For a packet to pass user validity check based on OUI MAC addresses, the sender MAC address must be an OUI MAC address and the voice VLAN must be enabled.)
4. If no match is found, the ARP packet is considered invalid and is discarded.

For more information about voice VLANs and OUI MAC addresses, see *Layer 2—LAN Switching Configuration Guide*.

Configuration guideliens

Follow these guidelines when you configure user validity check:

- Static IP source guard binding entries are created by using the **ip source binding** command. For more information, see "Configuring IP source guard."
- Dynamic DHCP snooping entries are automatically generated by DHCP snooping. For more information, see *Layer 3—IP Services Configuration Guide*.
- 802.1X security entries are generated by 802.1X. After a client passes 802.1X authentication and uploads its IP address to an ARP detection enabled device, the device automatically generates an 802.1X security entry. Therefore, the 802.1X client must be able to upload its IP address to the device. For more information, see "Configuring 802.1X."
- At least the configured rules, static IP source guard binding entries, DHCP snooping entries, or 802.1X security entries must be available for user validity check. Otherwise, ARP packets received from ARP untrusted ports will be discarded, except the ARP packets with an OUI MAC address as the sender MAC address when voice VLAN is enabled.

- You must specify a VLAN for an IP source guard binding entry. Otherwise, no ARP packets can match the IP source guard binding entry.

Configuration procedure

To configure user validity check:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set rules for user validity check.	**arp detection** *id-number* { **permit** | **deny** } **ip** { **any** | *ip-address* [*ip-address-mask*] } **mac** { **any** | *mac-address* [*mac-address-mask*] } [**vlan** *vlan-id*]	Optional. By default, no rule is configured.
3.	Enter VLAN view.	**vlan** *vlan-id*	N/A
4.	Enable ARP detection for the VLAN.	**arp detection enable**	ARP detection based on static IP source guard binding entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses is disabled by default.
5.	Return to system view.	**quit**	N/A
6.	Enter Layer 2 Ethernet interface/Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
7.	Configure the port as a trusted port on which ARP detection does not apply.	**arp detection trust**	Optional. The port is an untrusted port by default.

Configuring ARP packet validity check

Perform this task to 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-zero, all-one, or multicast IP addresses are considered invalid and the corresponding packets are discarded.

To configure ARP packet validity check:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter VLAN view.	**vlan** *vlan-id*	N/A

Step		Command	Remarks
3.	Enable ARP detection for the VLAN.	**arp detection enable**	Disabled by default.
4.	Return to system view.	**quit**	N/A
5.	Enable ARP packet validity check and specify the objects to be checked.	**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *	Disabled by default.
6.	Enter Layer 2 Ethernet port/Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
7.	Configure the port as a trusted port on which ARP detection does not apply.	**arp detection trust**	Optional. The port is an untrusted port by default.

Configuring ARP restricted forwarding

ARP restricted forwarding controls the forwarding of ARP packets that are received on untrusted ports and have passed ARP detection in the following cases:

- If the packets are ARP requests, they are forwarded through the trusted ports.
- If the packets are ARP responses, 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 ports.

Before performing the following configuration, make sure you have configured the **arp detection enable** command.

To enable ARP restricted forwarding:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter VLAN view.	**vlan** *vlan-id*	N/A
3.	Enable ARP restricted forwarding.	**arp restricted-forwarding enable**	Disabled by default

Displaying and maintaining ARP detection

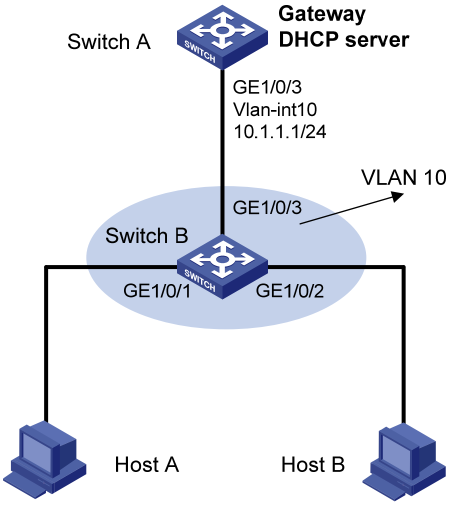
Task	Command	Remarks
Display the VLANs enabled with ARP detection.	**display arp detection** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the ARP detection statistics.	**display arp detection statistics** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear the ARP detection statistics.	**reset arp detection statistics** [**interface** *interface-type interface-number*]	Available in user view

User validity check configuration example

Network requirements

As shown in Figure 86, configure Switch B to perform user validity check based on 802.1X security entries for connected hosts.

Figure 86 Network diagram



Configuration procedure

1. Add all ports on Switch B into VLAN 10, and configure the IP address of VLAN-interface 10 on Switch A. (Details not shown.)
2. Configure Switch A as a DHCP server:

   # 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 and Host B as 802.1X clients and configure them to upload IP addresses for ARP detection. (Details not shown.)
4. Configure Switch B:

   # Enable the 802.1X function.

```
<SwitchB> system-view
[SwitchB] dot1x
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dot1x
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] dot1x
[SwitchB-GigabitEthernet1/0/2] quit
```

   # Add local access user **test**.

```
[SwitchB] local-user test
[SwitchB-luser-test] service-type lan-access
```

```
[SwitchB-luser-test] password simple test
[SwitchB-luser-test] quit
```

# Enable ARP detection for VLAN 10.

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp detection enable
```

# Configure the upstream port as a trusted port and the downstream ports as untrusted ports (a port is an untrusted port by default).

```
[SwitchB-vlan10] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] arp detection trust
[SwitchB-GigabitEthernet1/0/3] quit
```

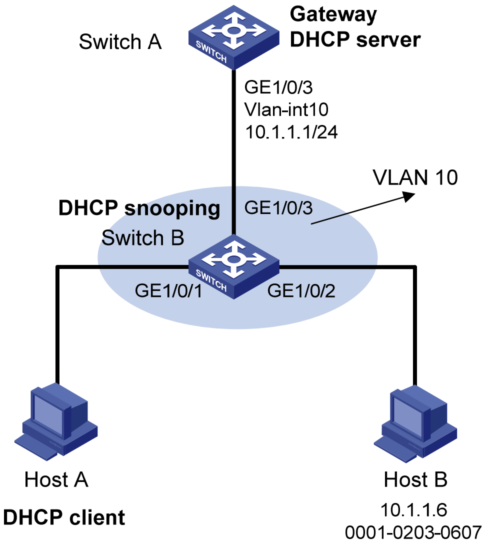
After the preceding configurations are complete, when ARP packets arrive at interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, they are checked against 802.1X security entries.

User validity check and ARP packet validity check configuration example

Network requirements

Configure Switch B to perform ARP packet validity check and user validity check based on static IP source guard binding entries and DHCP snooping entries for connected hosts.

Figure 87 Network diagram



Configuration procedure

1. Add all ports on Switch B to VLAN 10, and configure the IP address of VLAN-interface 10 on Switch A. (Details not shown.)
2. Configure DHCP address pool 0 on Switch A as a DHCP server.

```
<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 as DHCP client, and Host B as user. (Details not shown.)
4. Configure Switch B:

   # Enable DHCP snooping.

   ```
   <SwitchB> system-view
   [SwitchB] dhcp-snooping
   [SwitchB] interface gigabitethernet 1/0/3
   [SwitchB-GigabitEthernet1/0/3] dhcp-snooping trust
   [SwitchB-GigabitEthernet1/0/3] quit
   ```

   # Enable ARP detection for VLAN 10.

   ```
   [SwitchB] vlan 10
   [SwitchB-vlan10] arp detection enable
   ```

   # Configure the upstream port as a trusted port (a port is an untrusted port by default).

   ```
   [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 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
   ```

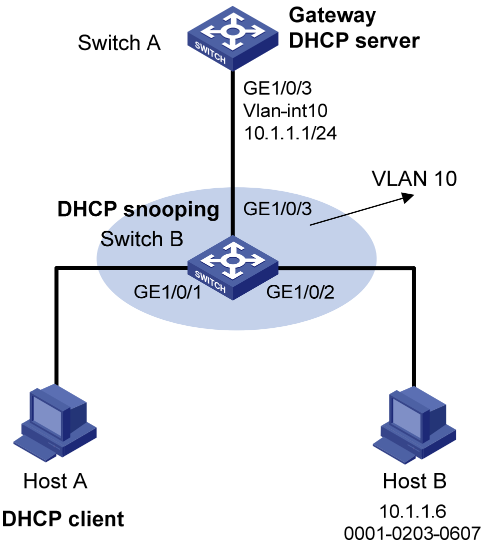
   After the configurations are completed, ARP packets received on interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 have their MAC and IP addresses checked first, and then are checked against the static IP source guard binding entries and finally DHCP snooping entries.

ARP restricted forwarding configuration example

Network requirements

As shown in Figure 88, configure ARP restricted forwarding on Switch B where ARP detection is configured so that port isolation configured on Switch B can take effect for broadcast ARP requests.

Figure 88 Network diagram



Configuration procedure

1. Configure VLAN 10, add ports to VLAN 10, and configure the IP address of the VLAN-interface, as shown in Figure 84. (Details not shown.)
2. Configure DHCP address pool 0 on Switch A as a DHCP server.

```
<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 the DHCP client on Hosts A and 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
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/3] quit
```

# Enable ARP detection.

```
[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 the checking of the MAC addresses and IP addresses of ARP packets.

```
[SwitchB] arp detection validate dst-mac ip src-mac
```

# Configure port isolation.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port-isolate enable
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port-isolate enable
[SwitchB-GigabitEthernet1/0/2] quit
```

After the preceding configurations are complete, ARP packets received on interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 have their MAC and IP addresses checked first, and then are checked against the static IP source guard binding entries and finally 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.

# Configure ARP restricted forwarding.

```
[SwitchB] vlan 10
[SwitchB-vlan10] arp restricted-forwarding enable
[SwitchB-vlan10] quit
```

After the configuration, Switch B forwards ARP broadcast requests from Host A to Switch A through the trusted port GigabitEthernet 1/0/3, and thus Host B cannot receive such packets. Port isolation works normally.

Configuring ARP automatic scanning and fixed ARP

ARP automatic scanning is usually used together with the fixed ARP feature.

With ARP automatic scanning enabled on an interface, the device automatically scans neighbors on the interface, sends ARP requests to the neighbors, obtains their MAC addresses, and creates dynamic ARP entries.

Fixed ARP allows the device to change the existing dynamic ARP entries (including those generated through ARP automatic scanning) into static ARP entries. The fixed ARP feature effectively prevents ARP entries from being modified by attackers.

HP recommends that you use ARP automatic scanning and fixed ARP in a small-scale network such as a cybercafe.

Configuration guidelines

Follow these guidelines when you configure ARP automatic scanning and fixed ARP:

- IP addresses existing in ARP entries are not scanned.
- ARP automatic scanning may 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 static ARP entries changed from dynamic ARP entries have the same attributes as the manually configured static ARP entries.
- Use the **arp fixup** command to change the existing dynamic ARP entries into static ARP entries. You can use this command again to change the dynamic ARP entries learned later into static ARP entries.

- The number of static ARP entries changed from dynamic ARP entries is restricted by the number of static ARP entries that the device supports. As a result, the device may fail to change all dynamic ARP entries into static ARP entries.
- To delete a specific static ARP entry changed from a dynamic one, use the **undo arp** *ip-address* command. To delete all such static ARP entries, use the **reset arp all** or **reset arp static** command.

Configuration procedure

To configure ARP automatic scanning and fixed ARP:

Step	Command
1. Enter system view.	**system-view**
2. Enter interface view.	**interface** *interface-type interface-number*
3. Enable ARP automatic scanning.	**arp scan** [*start-ip-address* **to** *end-ip-address*]
4. Return to system view.	**quit**
5. Enable fixed ARP.	**arp fixup**

Configuring ARP gateway protection

The ARP gateway protection feature, if configured on ports not connected with the gateway, can block gateway spoofing attacks.

When such a port 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 normally.

Configuration guidelines

Follow these guidelines when you configure ARP gateway protection:

- You can enable ARP gateway protection for up to eight gateways on a port.
- Commands **arp filter source** and **arp filter binding** cannot be both configured on a port.
- If ARP gateway protection works with ARP detection, and ARP snooping, ARP gateway protection applies first.

Configuration procedure

To configure ARP gateway protection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter Layer 2 Ethernet interface view/Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3. Enable ARP gateway protection for a specific gateway.	**arp filter source** *ip-address*	Disabled by default

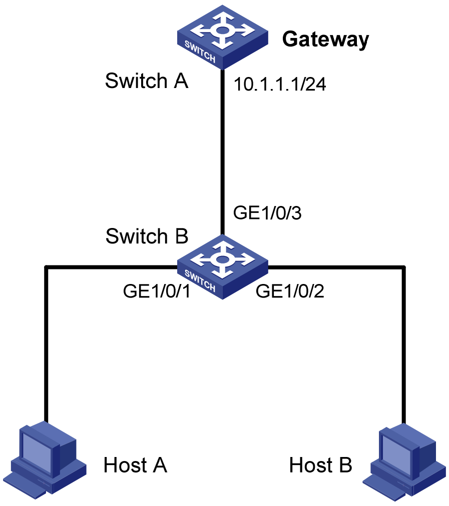
Configuration example

Network requirements

As shown in Figure 89, 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 89 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
```

After the configuration is complete, Switch B will discard the ARP packets whose source IP address is that of the gateway.

Configuring ARP filtering

To prevent gateway spoofing and user spoofing, the ARP filtering feature controls the forwarding of ARP packets on a port.

The port checks the sender IP and MAC addresses in a received ARP packet against configured ARP filtering entries. If a match is found, the packet is handled normally. If not, the packet is discarded.

Configuration guidelines

Follow these guidelines when you configure ARP filtering:

- You can configure up to eight ARP filtering entries on a port.
- Commands **arp filter source** and **arp filter binding** cannot be both configured on a port.

- If ARP filtering works with ARP detection, and ARP snooping, ARP filtering applies first.

Configuration procedure

To configure ARP filtering:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter Layer 2 Ethernet interface view/Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
3.	Configure an ARP filtering entry.	**arp filter binding** *ip-address mac-address*	Not configured by default

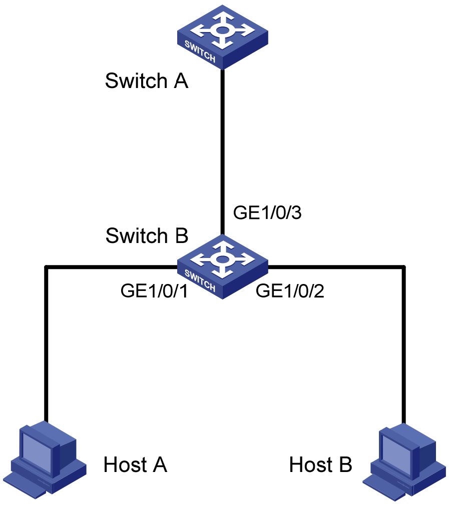
Configuration example

Network requirements

As shown in Figure 90, the IP and MAC addresses of Host A are 10.1.1.2 and 000f-e349-1233. The IP and MAC addresses of Host B are 10.1.1.3 and 000f-e349-1234.

Configure ARP filtering on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch B to permit specific ARP packets only.

Figure 90 Network diagram



Configuration procedure

# Configure ARP filtering on Switch B.

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] arp filter binding 10.1.1.2 000f-e349-1233
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

After the configuration is complete, GigabitEthernet 1/0/1 will permit incoming ARP packets with sender IP and MAC addresses as 10.1.1.2 and 000f-e349-1233, and discard other ARP packets. GigabitEthernet 1/0/2 will permit incoming ARP packets with sender IP and MAC addresses as 10.1.1.9 and 000f-e349-1233 and discard other ARP packets. ARP packets from Host A are permitted, but those from Host B are discarded.

Configuring ND attack defense

Overview

The IPv6 Neighbor Discovery (ND) protocol provides rich functions, such as address resolution, neighbor reachability detection, duplicate address detection, router/prefix discovery and address autoconfiguration, and redirection. However, it does not provide any security mechanisms. Attackers can easily exploit the ND protocol to attack hosts and gateways by sending forged packets. For more information about the five functions of the ND protocol, see *Layer 3—IP Services Configuration Guide*.

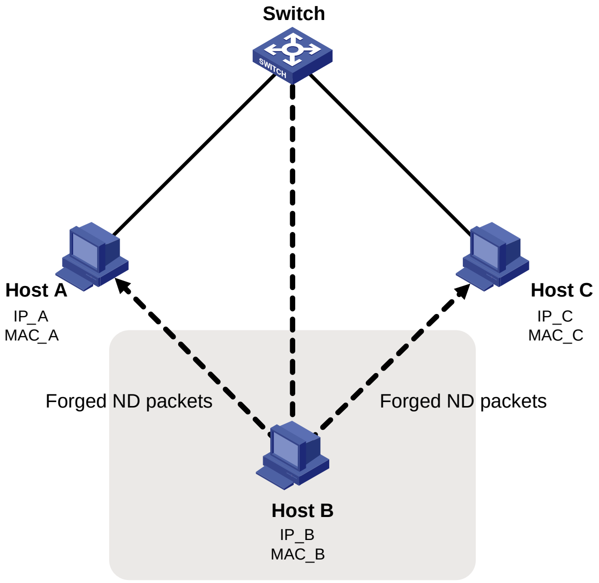
The ND protocol implements its function by using five types of ICMPv6 messages:

- Neighbor Solicitation (NS)
- Neighbor Advertisement (NA)
- Router Solicitation (RS)
- Router Advertisement (RA)
- Redirect (RR)

As shown in Figure 91, an attacker can attack a network by sending forged ICMPv6 messages:

- Sends forged NS/NA/RS packets with the IPv6 address of a victim host. The gateway and other hosts update the ND entry for the victim host with incorrect address information. As a result, all packets intended for the victim host are sent to the attacking host rather than the victim host.
- Sends forged RA packets 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 91 ND attack diagram



All forged ND packets have two common features:

- The Ethernet frame header and the source link layer address option of the ND packet contain different source MAC addresses.

- The mapping between the source IPv6 address and the source MAC address in the Ethernet frame header is invalid.

To identify forged ND packets, HP developed the source MAC consistency check and ND detection.

Enabling source MAC consistency check for ND packets

Use source MAC consistency check on a gateway to filter out ND packets that carry different source MAC addresses in the Ethernet frame header and the source link layer address option.

To enable source MAC consistency check for ND packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable source MAC consistency check for ND packets.	**ipv6 nd mac-check enable**	Disabled by default

Configuring the ND detection function

Introduction to ND detection

Use the ND detection function on access devices to verify the source of ND packets. If an ND packet comes from a spoofing host or gateway, it is discarded.

The ND detection function operates on a per VLAN basis. In an ND detection-enabled VLAN, a port is either ND-trusted or ND-untrusted:

- An ND-trusted port does not check ND packets for address spoofing.
- An ND-untrusted port checks all ND packets but RA and RR messages in the VLAN for source spoofing. RA and RR messages are considered illegal and are discarded directly.

The ND detection function checks an ND packet by looking up the IPv6 static bindings table of the IP source guard function, ND snooping table, and DHCPv6 snooping table in the following steps:

1. Looks up the IPv6 static binding table of IP source guard, based on the source IPv6 address and the source MAC address in the Ethernet frame header of the ND packet. If an exact match is found, the ND packet is forwarded. If an entry matches the source IPv6 address but not the source MAC address, the ND packet is discarded. If no entry matches the source IPv6 address, the ND detection function continues to look up the DHCPv6 snooping table and the ND snooping table.
2. If an exact match is found in either the DHCPv6 snooping or ND snooping table, the ND packet is forwarded. If no match is found in either table, the packet is discarded. If neither the DHCPv6 snooping table nor the ND snooping table is available, the ND packet is discarded.

Configuration guidelines

Follow these guidelines when you configure ND detection:

- To create IPv6 static bindings with IP source guard, use the **ipv6 source binding** command. For more information, see "Configuring IP source guard."

- The DHCPv6 snooping table is created automatically by the DHCPv6 snooping module. For more information, see *Layer 3—IP Services Configuration Guide*.
- The ND snooping table is created automatically by the ND snooping module. For more information, see *Layer 3—IP Services Configuration Guide*.
- ND detection performs source check by using the binding tables of IP source guard, DHCPv6 snooping, and ND snooping. To prevent an ND-untrusted port from discarding legal ND packets in an ND detection-enabled VLAN, make sure that at least one of the three functions is available.
- When creating an IPv6 static binding with IP source guard for ND detection in a VLAN, specify the VLAN ID for the binding. If not, no ND packets in the VLAN can match the binding.
- The ND detection function does not check ND packets containing link local addresses.

Configuration procedure

To configure ND detection:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter VLAN view.	**vlan** *vlan-id*	N/A
3.	Enable ND Detection.	**ipv6 nd detection enable**	Disabled by default.
4.	Quit system view.	**quit**	N/A
5.	Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view.	**interface** *interface-type interface-number*	N/A
6.	Configure the port as an ND-trusted port.	**ipv6 nd detection trust**	Optional. A port does not trust sources of ND packets by default.

Displaying and maintaining ND detection

Task	Command	Remarks
Display the ND detection configuration.	**display ipv6 nd detection** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the statistics of discarded packets when the ND detection checks the user legality.	**display ipv6 nd detection statistics** [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Clear the statistics by ND detection.	**reset ipv6 nd detection statistics** [**interface** *interface-type interface-number*]	Available in user view

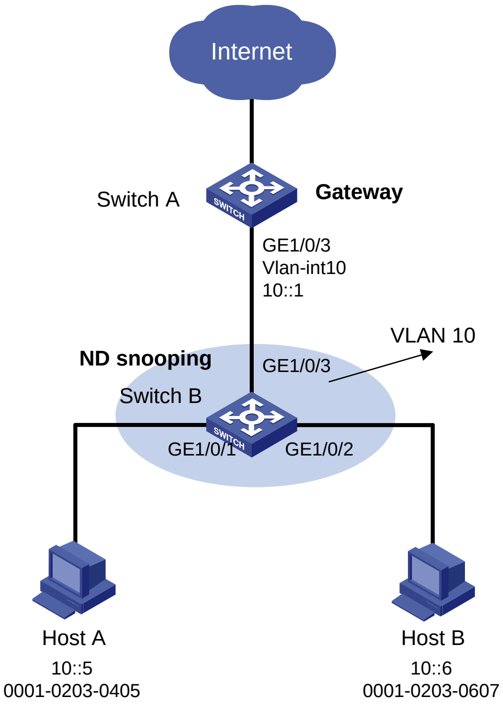
ND detection configuration example

Network requirements

As shown in Figure 92, Host A and Host B connect to Switch A, the gateway, through Switch B. Host A has the IPv6 address 10::5 and MAC address 0001-0203-0405. Host B has the IPv6 address 10::6 and MAC address 0001-0203-0607.

Enable ND detection on Switch B to filter out forged ND packets.

Figure 92 Network diagram



Configuration procedure

1. Configuring Switch A:

# Enable IPv6 forwarding.

```
<SwitchA> system-view
[SwitchA] ipv6
```

# Create VLAN 10.

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
```

# Assign port GigabitEthernet 1/0/3 to VLAN 10.

```
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchA-GigabitEthernet1/0/3] quit
```

# Assign an IPv6 address to VLAN-interface 10.

```
[SwitchA] interface vlan-interface 10
```

```
[SwitchA-Vlan-interface10] ipv6 address 10::1/64
[SwitchA-Vlan-interface10] quit
```

2. Configuring Switch B:

# Enable IPv6 forwarding.

```
<SwitchB> system-view
[SwitchB] ipv6
```

# Create VLAN 10.

```
[SwitchB] vlan 10
[SwitchB-vlan10] quit
```

# Add ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 10.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port access vlan 10
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port access vlan 10
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-type trunk
[SwitchB-GigabitEthernet1/0/3] port trunk permit vlan 10
[SwitchB-GigabitEthernet1/0/3] quit
```

# Enable ND snooping for global unicast and link local addresses in VLAN 10.

```
[SwitchB] ipv6 nd snooping enable link-local
[SwitchB] ipv6 nd snooping enable global
[SwitchB] vlan 10
[SwitchB-vlan 10] ipv6 nd snooping enable
```

# Enable ND detection in VLAN 10.

```
[SwitchB-vlan 10] ipv6 nd detection enable
[SwitchB-vlan 10] quit
```

# Configure the uplink port GigabitEthernet 1/0/3 as an ND-trusted port, and the downlink ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as ND-untrusted ports (the default).

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ipv6 nd detection trust
```

The configuration enables Switch B to check all incoming ND packets of ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 based on the ND snooping table.

Configuring SAVI

Overview

Source Address Validation (SAVI) is applied on access devices. SAVI creates a table of bindings between addresses and ports through other features such as ND snooping, DHCPv6 snooping, and IP Source Guard, and uses those bindings to check the validity of the source addresses of DHCPv6 protocol packets, ND protocol packets, and IPv6 data packets.

SAVI can be used in the following address assignment scenarios:

- DHCPv6-only: The hosts connected to the SAVI-enabled device obtain addresses only through DHCPv6.
- SLAAC-only: The hosts connected to the SAVI-enabled device obtain addresses only through Stateless Address Autoconfiguration (SLAAC).
- DHCPv6+SLAAC: The hosts connected to the SAVI-enabled device obtain addresses through DHCPv6 and SLAAC.

The following section describes SAVI configurations in these address assignment scenarios.

After a port is down, the switch can wait for a period of delay time before deleting the DHCPv6 snooping entries and ND snooping entries for that port. The deletion delay time is configurable. This delay ensures a valid IPv6 user to access the port for the event that a port goes down and resumes during that period.

Configuring global SAVI

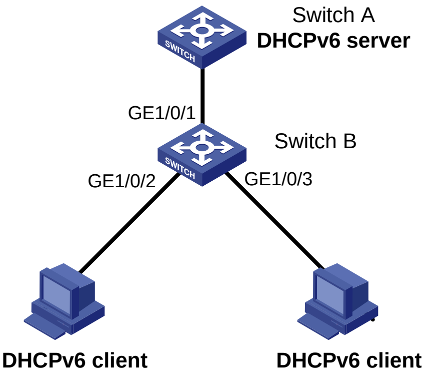
Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the SAVI function.	**ipv6 savi strict**	Disabled by default.
3. Setting the deletion delay time for SAVI.	**ipv6 savi down-delay** *time*	The default setting is 30 seconds.
4. Set the time to wait for a duplicate address detection (DAD) NA.	**ipv6 savi dad-delay** *value*	Optional One second by default. If no DAD NA is received within the specified time when the corresponding ND snooping entry is in detect state, the ND snooping entry changes to bound state.

Step	Command	Remarks
5. Set the time to wait for a DAD NS from a DHCPv6 client.	**ipv6 savi dad-preparedelay** *value*	Optional One second by default. This command is used with the DHCPv6 snooping function. After DHCPv6 snooping detects that a client obtains an IPv6 address, it monitors whether the client detects IP address conflict. If DHCPv6 snooping does not receive any DAD NS from the client before the set time expires, SAVI sends a DAD NS on behalf of the client.

SAVI configuration in DHCPv6-only address assignment scenario

Network requirements

Figure 93 Network diagram



As shown in Figure 93, Switch A is the DHCPv6 server. Switch B connects to the DHCPv6 server through interface GigabitEthernet 1/0/1, and connects to two DHCPv6 clients through interfaces GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3. The three interfaces of Switch B belong to VLAN 2. The client can obtain IP address only through DHCPv6. Configure SAVI on Switch B to automatically bind the IP addresses assigned through DHCPv6 and permit only packets from bound addresses and link-local addresses.

Configuration considerations

Configure Switch B as follows:

1. Enable SAVI.
2. Enable DHCPv6 snooping. For more information about DHCPv6 snooping, see *Layer 3—IP Services Configuration Guide*.
3. Enable link-local address ND snooping. For more information about ND snooping, see *Layer 3—IP Services Configuration Guide*.

4. Enable ND detection in VLAN 2 to check the ND packets arrived on the ports. For more information about ND detection, see "Configuring ND attack defense."
5. Configure a static IPv6 source guard binding entry on each interface connected to a client. This step is optional. If this step is not performed, SAVI does not check packets against static binding entries. For more information about static IPv6 source guard binding entries, see "Configuring IP source guard."
6. Configure dynamic IPv6 source guard binding on the interfaces connected to the clients. For more information about dynamic IPv6 source guard binding, see "Configuring IP source guard."

Packet check principles

Switch B checks DHCPv6 protocol packets from DHCPv6 clients against link-local address ND snooping entries, checks ND protocol packets against link-local address ND snooping entries, DHCPv6 snooping entries, and static binding entries, and checks the IPv6 data packets from the clients against dynamic binding entries (including link-local address ND snooping entries and DHCPv6 snooping entries) applied on the interfaces connected to the clients and against static binding entries. The items to be examined include MAC address, IPv6 address, VLAN information, and ingress port.

Configuration procedure

# Enable SAVI.

```
<SwitchB> system-view
[SwitchB] ipv6 savi strict
```

# Enable IPv6.

```
[SwitchB] ipv6
```

# Globally enable DHCPv6 snooping.

```
[SwitchB] ipv6 dhcp snooping enable
```

# Assign interfaces GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3
```

# Enable DHCPv6 snooping in VLAN 2.

```
[SwitchB-vlan2] ipv6 dhcp snooping vlan enable
[SwitchB] quit
```

# Configure interface GigabitEthernet 1/0/1 as a DHCP snooping trusted port.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

# Enable link-local address ND snooping and ND detection.

```
[SwitchB] ipv6 nd snooping enable link-local
[SwitchB] vlan 2
[SwitchB-vlan2] ipv6 nd snooping enable
[SwitchB-vlan2] ipv6 nd detection enable
[SwitchB-vlan2] quit
```

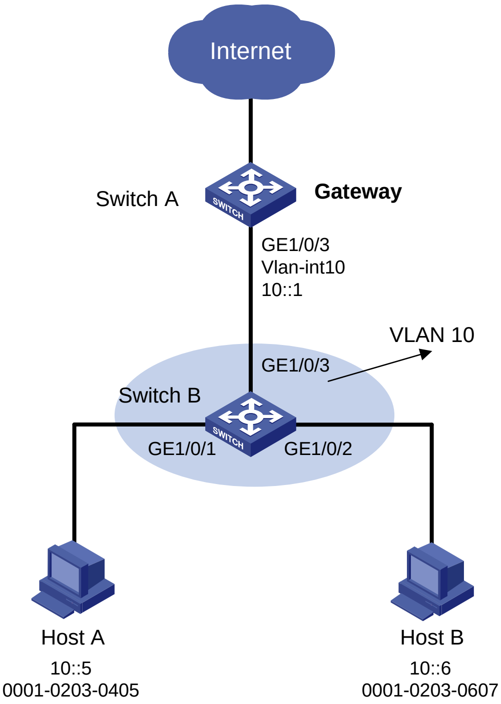
# Configure the dynamic IPv6 source guard binding function on downlink ports GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ipv6 verify source ipv6-address mac-address
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ipv6 verify source ipv6-address mac-address
[SwitchB-GigabitEthernet1/0/3] quit
```

SAVI configuration in SLAAC-only address assignment scenario

Network requirements

Figure 94 Network diagram



As shown in Figure 94, Switch A serves as the gateway. Switch B connects Host A and Host B. The hosts can obtain IPv6 addresses only through SLAAC. Configure SAVI on Switch B to bind the addresses assigned through SLAAC and permit only packets from the bound addresses.

Configuration considerations

Configure Switch B as follows:

1. Enable SAVI.
2. Enable global unicast address ND snooping and link-local address ND snooping. For more information about ND snooping, see *Layer 3—IP Services Configuration Guide*.
3. Enable ND detection in VLAN 10 to check the ND packets arrived on the ports. For more information about ND detection, see "Configuring ND attack defense."

4. Configure a static IPv6 source guard binding entry on each interface connected to a host. This step is optional. If this step is not performed, SAVI does not check packets against static binding entries. For more information about static IPv6 source guard binding entries, see "Configuring IP source guard."
5. Configure dynamic IPv6 source guard binding on the interfaces connected to the hosts. For more information about dynamic IPv6 source guard binding, see "Configuring IP source guard."
6. Enable DHCPv6 snooping and leave the interface connected to the gateway as its default status (non-trusted port) so that the hosts cannot obtain IP addresses through DHCPv6. For more information about DHCPv6 snooping, see *Layer 3—IP Services Configuration Guide*.

Packet check principles

Switch B checks ND protocol packets against ND snooping entries and static binding entries, and checks the IPv6 data packets from the hosts against dynamic binding entries (including ND snooping entries) applied on the interfaces connected to the hosts and against static binding entries. The items to be examined include MAC address, IPv6 address, VLAN information, and ingress port.

Configuration procedure

# Enable SAVI.

```
<SwitchB> system-view
[SwitchB] ipv6 savi strict
```

# Enable IPv6.

```
[SwitchB] ipv6
```

# Assign GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to VLAN 10.

```
[SwitchB] vlan 10
[SwitchB-vlan10] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3
[SwitchB-vlan10] quit
```

# Enable global unicast address ND snooping and link-local address ND snooping.

```
[SwitchB] ipv6 nd snooping enable link-local
[SwitchB] ipv6 nd snooping enable global
[SwitchB] vlan 10
[SwitchB-vlan10] ipv6 nd snooping enable
```

# Enable ND detection.

```
[SwitchB-vlan10] ipv6 nd detection enable
[SwitchB-vlan10] quit
```

# Enable DHCPv6 snooping.

```
[SwitchB] ipv6 dhcp snooping enable
```

# Configure uplink port GigabitEthernet 1/0/3 as an ND trusted port.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ipv6 nd detection trust
[SwitchB-GigabitEthernet1/0/3] quit
```

# Configure the dynamic IPv6 source guard binding function on downlink ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

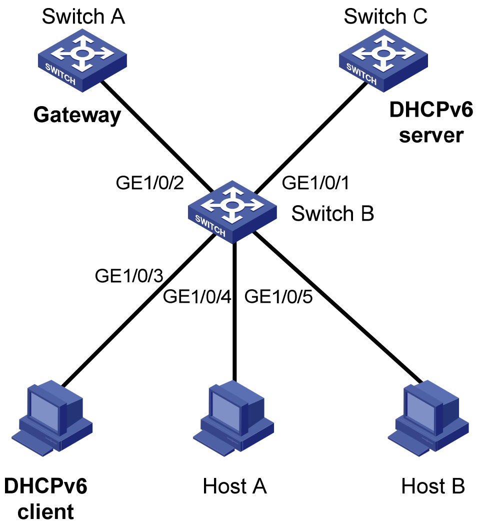
```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ipv6 verify source ipv6-address mac-address
```

```
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ipv6 verify source ipv6-address mac-address
[SwitchB-GigabitEthernet1/0/2] quit
```

SAVI configuration in DHCPv6+SLAAC address assignment scenario

Network requirements

Figure 95 Network diagram



As shown in Figure 95, Switch B connects to the DHCPv6 server through interface GigabitEthernet 1/0/1 and connects to the DHCPv6 client through interface GigabitEthernet 1/0/3. Host A and Host B access Gateway (Switch A) through Switch B. Interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 on Switch B belong to VLAN 2. The hosts can obtain IP addresses through DHCPv6 or SLAAC. Configure SAVI on Switch B to permit only packets from addresses assigned through DHCPv6 and the bound addresses assigned through SLAAC.

Configuration considerations

Configure Switch B as follows:

1. Enable SAVI.
2. Enable DHCPv6 snooping. For more information about DHCPv6 snooping, see *Layer 3—IP Services Configuration Guide*.
3. Enable global unicast address ND snooping and link-local address ND snooping. For more information about ND snooping, see *Layer 3—IP Services Configuration Guide*.
4. Enable ND detection in VLAN 2 to check the ND packets arrived on the ports. For more information about ND detection, see "Configuring ND attack defense."
5. Configure a static IPv6 source guard binding entry on each interface connected to a host. This step is optional. If this step is not performed, SAVI does not check packets against static binding entries.

For more information about static IPv6 source guard binding entries, see "Configuring IP source guard."

6. Configure dynamic IPv6 source guard binding on the interfaces connected to the hosts. For more information about dynamic IPv6 source guard binding, see "Configuring IP source guard."

Packet check principles

Switch B checks DHCPv6 protocol packets from DHCPv6 clients against link-local address ND snooping entries, checks ND protocol packets against ND snooping entries, DHCPv6 snooping entries, and static binding entries, and checks the IPv6 data packets from the hosts against dynamic binding entries (including ND snooping entries and DHCPv6 snooping entries) applied on the interfaces connected to the hosts and against static binding entries. The items to be examined include MAC address, IPv6 address, VLAN information, and ingress port.

Configuration procedure

# Enable SAVI.

```
<SwitchB> system-view
[SwitchB] ipv6 savi strict
```

# Enable IPv6.

```
[SwitchB] ipv6
```

# Enable DHCPv6 snooping.

```
[SwitchB] ipv6 dhcp snooping enable
```

# Assign interfaces GigabitEthernet 1/0/1 through GigabitEthernet 1/0/5 to VLAN 2.

```
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2 gigabitethernet 1/0/3
gigabitethernet 1/0/4 gigabitethernet 1/0/5
```

# Enable DHCPv6 snooping in VLAN 2.

```
[SwitchB-vlan2] ipv6 dhcp snooping vlan enable
[SwitchB] quit
```

# Configure interface GigabitEthernet 1/0/1 as a DHCPv6 snooping trusted port.

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

# Enable ND snooping and ND detection.

```
[SwitchB] ipv6 nd snooping enable link-local
[SwitchB] ipv6 nd snooping enable global
[SwitchB] vlan 2
[SwitchB-vlan2] ipv6 nd snooping enable
[SwitchB-vlan2] ipv6 nd detection enable
[SwitchB-vlan2] quit
```

# Configure interface GigabitEthernet 1/0/2 as an ND detection trusted port.

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ipv6 nd detection trust
[SwitchB-GigabitEthernet1/0/2] quit
```

Configure the dynamic IPv6 source guard binding function on downlink ports GigabitEthernet 1/0/3 through GigabitEthernet 1/0/5.

```
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] ipv6 verify source ipv6-address mac-address
[SwitchB-GigabitEthernet1/0/3] quit
[SwitchB] interface gigabitethernet 1/0/4
[SwitchB-GigabitEthernet1/0/4] ipv6 verify source ipv6-address mac-address
[SwitchB-GigabitEthernet1/0/4] quit
[SwitchB] interface gigabitethernet 1/0/5
[SwitchB-GigabitEthernet1/0/5] ipv6 verify source ipv6-address mac-address
```

Configuring blacklist

Overview

The blacklist feature is an attack prevention mechanism that filters packets based on the source IP address. Compared with ACL-based packet filtering, the blacklist feature is easier to configure and fast in filtering packets sourced from particular IP addresses.

The device can dynamically add and remove blacklist entries by cooperating with the login user authentication feature. When the device detects that a user tried to use FTP, Telnet, SSH, SSL, or web to log in to the device for a specific number of times but failed to log in, it considers the user an invalid user and automatically blacklists the user's IP address to filter subsequent packets sourced from that IP address. This function can effectively prevent users from cracking passwords by repeatedly trying to log in.

The device always uses the login failure threshold of 6 and sets the aging time of a dynamic blacklist entry to 10 minutes. These two settings are not configurable. User login failure reasons include wrong username, wrong password, and wrong verification code (for web users).

The device also supports adding and removing blacklist entries manually. Manually configured blacklist entries fall into two categories: permanent and non-permanent. A permanent blacklist entry is always present unless being removed manually, whereas a non-permanent blacklist entry has a limited lifetime depending on your configuration. When the lifetime of a non-permanent entry expires, the device removes the entry from the blacklist, allowing the packets of the IP address defined by the entry to pass through.

Configuring the blacklist feature

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the blacklist feature.	**blacklist enable**	Disabled by default.
3. Add a blacklist entry.	**blacklist ip** *source-ip-address* [**timeout** *minutes*]	Optional. To add a permanent entry, do not specify the **timeout** *minutes* option.

Displaying and maintaining the blacklist

Task	Command	Remarks
Display blacklist information.	**display blacklist** { **all** | **ip** *source-ip-address* [**slot** *slot-number*] | **slot** *slot-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

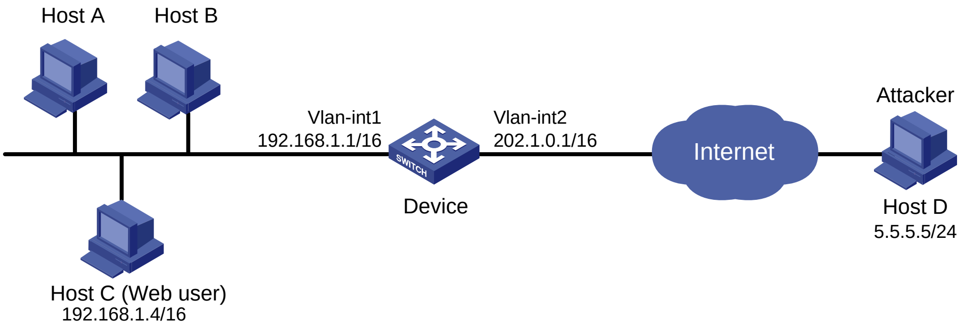
Blacklist configuration example

Network requirements

As shown in Figure 96, Host A, Host B, and Host C are internal users, and external user Host D is considered an attacker.

Configure Device to always filter packets from Host D, and to prevent internal users from guessing passwords.

Figure 96 Network diagram



Configuration procedure

# Assign IP addresses to the interfaces of Device. (Details not shown.)

# Enable the blacklist feature.

```
<Device> system-view
[Device] blacklist enable
```

# Add the IP address of Host D 5.5.5.5 to the blacklist. Do not specify any aging time to make the entry never age out.

```
[Device] blacklist ip 5.5.5.5
```

Verifying the configuration

If Host C tries to log in to Device through web for six times but fails to log in, the device blacklists Host C. Use the **display blacklist all** command to view all added blacklist entries.

```
[Device] display blacklist all
                    Blacklist information
------------------------------------------------------------------------------
Blacklist                               : enabled
Blacklist items                         : 2
------------------------------------------------------------------------------
IP              Type   Aging started       Aging finished      Dropped packets
                       YYYY/MM/DD hh:mm:ss YYYY/MM/DD hh:mm:ss
5.5.5.5         manual 2011/04/09 16:02:20 Never               0
192.168.1.4     manual 2011/04/09 16:02:26 2011/04/09 16:12:26 0
```

Host D and Host C are on the blacklist. Host C will stay on the list for 10 minutes, and will then be able to try to log in again. The entry for Host D will never age out. When you do not consider Host D an attacker anymore, you can use the **undo blacklist ip 5.5.5.5** command to remove the entry.

Configuring FIPS

Overview

Federal Information Processing Standards (FIPS), developed by the National Institute of Standard and Technology (NIST) of the United States, specify the requirements for cryptography modules. FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4" from low to high. Currently, the switch supports Level 2.

Unless otherwise noted, *FIPS* in the document refers to FIPS 140-2.

FIPS self-tests

When the device operates in FIPS mode, it has self-test mechanisms, including the power-up self-test and conditional self-tests, to ensure the normal operation of cryptography modules. You can also trigger a self-test. If a self-test fails, the device restarts.

△ CAUTION:

If the switch reboots repeatedly, it might be caused by software failures or hardware damages. Contact technical support engineers to upgrade the software or repair the damaged hardware.

Power-up self-test

The power-up self-test, also called "known-answer test", examines the availability of FIPS-allowed cryptographic algorithms. 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 known-answer test fails.

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:

- **Pair-wise consistency test**—This test is run when a DSA/RSA asymmetrical key-pair is generated. It uses the public key to encrypt a plain text, and uses the private key to decrypt the encrypted text. If the decryption is successful, the test succeeds. Otherwise, the test fails.
- **Continuous random number generator test**—This test is run when a random number is generated in FIPS mode. If two consecutive random numbers are different, the test succeeds. Otherwise, the test fails.

Triggering a self-test

To examine whether the cryptography modules operate normally, you can use a command to 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 automatically reboots.

Configuration procedure

To configure FIPS, complete the following tasks:

1. Remove the existing key pairs and certificates.
2. Enable the FIPS mode.
3. Enable the password control function.
4. Configure local user attributes (including local username, service type, password, and so on) on the switch.
5. Save the configuration.

After you finish the above configurations, reboot the switch. The switch works in FIPS mode that complies with the FIPS 140-2 standard after it starts up. For Common Criteria (CC) evaluation in FIPS mode, the switch also works in a operating mode that complies with the CC standard.

The switch does not support an upgrade from a FIPS-incompatible version to a FIPS-compatible version.

Enabling the FIPS mode

You must reboot the switch after you enable or disable the FIPS mode to make your configuration take effect. If you change the FIPS mode for an IRF fabric, you must reboot all IRF member devices.

After you change the switch to operate in FIPS mode, local Telnet users in previous non-FIPS cannot log into the switch.

Do not disable the password control function when the switch operates in FIPS mode. Otherwise, users might be unable to log in.

To enable the FIPS mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the FIPS mode.	**fips mode enable**	Disabled by default.

After you enable the FIPS mode and reboot the switch, the switch works in FIPS mode after it starts up and the following changes occur.

- FTP/TFTP is disabled.
- Telnet is disabled.
- The HTTP server is disabled.
- Cluster management is disabled.
- SNMPv1 and SNMPv2c are disabled. Only SNMPv3 is available.
- The SSL server only supports TLS1.0.
- The SSH server does not support SSHv1 clients.
- SSH only supports RSA.
- The generated RSA key pairs must have a modulus length of 2048 bits. The generated DSA key pair must have a modulus of at least 1024 bits.
- SSH, SNMPv3, IPsec, and SSL do not support DES, 3DES, RC4, or MD5.

Triggering a self-test

To examine whether the cryptography modules operate normally, you can use a command to 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 automatically reboots.

To trigger a self-test:

Step	Command
1. Enter system view.	**system-view**
2. Trigger a self-test.	**fips self-test**

Displaying and maintaining FIPS

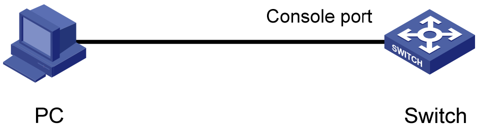
Task	Command	Remarks
Display FIPS mode state.	**display fips status**	Available in any view.

FIPS configuration example

Network requirements

PC connects to Switch through a console port. Configure Switch to operate in FIPS mode and create a local user for PC so that PC can log in to the switch.

Figure 97 Network diagram



Configuration procedure

# Enable the FIPS mode.

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue?[Y/N]:y
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.
```

# Enable the password control function.

```
[Sysname] password-control enable
```

# Create a local user named **test**, and set its service type as **terminal**, privilege level as **3**, and password as **AAbbcc1234%**. The password is a string of at least 10 characters by default and must contain both uppercase and lowercase letters, digits, and special characters.

```
[Sysname] local-user test
```

```
[Sysname-luser-test] service-type terminal
[Sysname-luser-test] authorization-attribute level 3
[Sysname-luser-test] password
Password:***********
Confirm :***********
Updating user(s) information, please wait...........
[Sysname-luser-test] quit
```

# Save the configuration.

```
[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 mainboard device successfully.
 Configuration is saved to device successfully.
[Sysname] quit
```

# Reboot the switch.

```
<Sysname> reboot
```

CAUTION:

If you do not create a local user and its password before you reboot the switch, you cannot log in to the switch after the switch reboots. In this case, reboot the switch without the configuration file (by ignoring or removing the configuration file) so that the switch operates in non-FIPS mode, and then make correct configurations.

Verifying the configuration

After the switch reboots, enter the username (test) and password (AAbbcc1234%). The system prompts that your first login is successful, and asks you to enter a new password. Enter a new password which has at least four characters different than the previous one and confirm the password. Then, the system displays the <Sysname> prompt.

```
User interface aux0 is available.

Please press ENTER.

Login authentication

Username:test
Password:
Info: First logged in. For security reasons you will need to change your password.
 Please enter your new password.
Password:**********
Confirm :**********
Updating user(s) information, please wait...........
<Sysname>
```

# Display the current FIPS mode. You can see that the FIPS mode is enabled.

```
<Sysname> display fips status
 FIPS mode is enabled
```

Support and other resources

Contacting HP

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

http://www.hp.com/support

Before contacting HP, collect the following information:

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

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

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

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

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

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

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

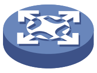
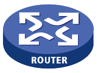
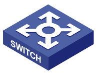
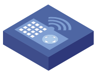
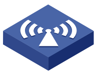
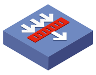
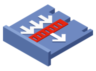
GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ CAUTION	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.
❗ IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
💡 TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	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.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index