

HP A5120 EI Switch Series Security

Configuration Guide

Abstract

This document describes the software features for the HP A Series products and guides you through the software configuration procedures. These configuration guides also provide configuration examples to help you apply software features to different network scenarios.

This documentation is intended for network planners, field technical support and servicing engineers, and network administrators working with the HP A Series products.

Part number: 5998-1800
Software version: Release 2208
Document version: 5W100-20110530



Legal and notice information

© Copyright 2011 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

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

| | |
|--|----|
| AAA configuration | 1 |
| AAA overview | 1 |
| RADIUS | 2 |
| HWTACACS | 7 |
| Domain-based user management | 9 |
| RADIUS server feature of the device | 10 |
| Protocols and standards | 11 |
| RADIUS attributes | 11 |
| AAA configuration considerations and task list | 14 |
| Configuring AAA schemes | 16 |
| Configuring local users | 16 |
| Configuring RADIUS schemes | 20 |
| Configuring HWTACACS schemes | 30 |
| Configuring AAA methods for ISP domains | 36 |
| Configuration prerequisites | 36 |
| Creating an ISP domain | 36 |
| Configuring ISP domain attributes | 36 |
| Configuring AAA authentication methods for an ISP domain | 37 |
| Configuring AAA authorization methods for an ISP domain | 39 |
| Configuring AAA accounting methods for an ISP domain | 40 |
| Tearing down user connections forcibly | 42 |
| Configuring a network device as a RADIUS server | 42 |
| RADIUS server functions configuration task list | 42 |
| Configuring a RADIUS user | 42 |
| Specifying a RADIUS client | 43 |
| Displaying and maintaining AAA | 44 |
| AAA configuration examples | 44 |
| AAA for Telnet users by an HWTACACS server | 44 |
| AAA for Telnet users by separate servers | 45 |
| Authentication/Authorization for SSH/Telnet users by a RADIUS server | 47 |
| AAA for 802.1X users by a RADIUS server | 50 |
| Level switching authentication for Telnet users by an HWTACACS server | 56 |
| RADIUS authentication and authorization for Telnet users by a network device | 59 |
| Troubleshooting AAA | 61 |
| Troubleshooting RADIUS | 61 |
| Troubleshooting HWTACACS | 62 |
| 802.1X fundamentals | 63 |
| 802.1X architecture | 63 |
| Controlled/uncontrolled port and port authorization status | 63 |
| 802.1X-related protocols | 64 |
| Packet format | 64 |
| EAP over RADIUS | 66 |
| Initiating 802.1X authentication | 66 |
| 802.1X client as the initiator | 66 |
| Access device as the initiator | 66 |
| 802.1X authentication procedures | 67 |
| A comparison of EAP relay and EAP termination | 67 |
| EAP relay | 68 |
| EAP termination | 69 |

| | |
|--|-----|
| 802.1X configuration | 71 |
| HP implementation of 802.1X | 71 |
| Access control methods | 71 |
| Using 802.1X authentication with other features | 71 |
| Configuring 802.1X | 74 |
| Configuration prerequisites | 74 |
| 802.1X configuration task list | 74 |
| Enabling 802.1X | 75 |
| Specifying EAP relay or EAP termination | 75 |
| Setting the port authorization state | 76 |
| Specifying an access control method | 77 |
| Setting the maximum number of concurrent 802.1X users on a port | 77 |
| Setting the maximum number of authentication request attempts | 78 |
| Setting the 802.1X authentication timeout timers | 78 |
| Configuring the online user handshake function | 78 |
| Configuring the authentication trigger function | 79 |
| Specifying a mandatory authentication domain on a port | 80 |
| Enabling the quiet timer | 81 |
| Enabling the periodic online user re-authentication function | 81 |
| Configuring an 802.1X guest VLAN | 82 |
| Configuring an Auth-Fail VLAN | 83 |
| Displaying and maintaining 802.1X | 84 |
| 802.1X configuration examples | 84 |
| 802.1X authentication configuration example | 84 |
| 802.1X with guest VLAN and VLAN assignment configuration example | 86 |
| 802.1X with ACL assignment configuration example | 89 |
| EAD fast deployment configuration | 91 |
| EAD fast deployment overview | 91 |
| EAD fast deployment implementation | 91 |
| Configuring EAD fast deployment | 91 |
| Configuration prerequisites | 91 |
| Configuration procedure | 91 |
| Displaying and maintaining EAD fast deployment | 92 |
| EAD fast deployment configuration example | 93 |
| Troubleshooting EAD fast deployment | 95 |
| Web browser users cannot be correctly redirected | 95 |
| MAC authentication configuration | 96 |
| MAC authentication overview | 96 |
| User account policies | 96 |
| Authentication approaches | 96 |
| MAC authentication timers | 97 |
| Using MAC authentication with other features | 97 |
| VLAN assignment | 97 |
| ACL assignment | 97 |
| Guest VLAN | 97 |
| MAC authentication configuration task list | 98 |
| Basic configuration for MAC authentication | 98 |
| Configuration prerequisites | 98 |
| Configuration procedure | 98 |
| Specifying an authentication domain for MAC authentication users | 99 |
| Configuring a MAC authentication guest VLAN | 100 |
| Configuration prerequisites | 100 |
| Configuration procedure | 100 |
| Displaying and maintaining MAC authentication | 101 |

| | |
|---|------------|
| MAC authentication configuration examples | 101 |
| Local MAC authentication configuration example | 101 |
| RADIUS-based MAC authentication configuration example | 103 |
| ACL assignment configuration example | 105 |
| Portal configuration | 108 |
| Portal overview | 108 |
| Introduction to portal | 108 |
| Extended portal functions | 108 |
| Portal system components | 108 |
| Portal system using the local portal server | 110 |
| Portal authentication modes | 111 |
| Layer 2 portal authentication process | 111 |
| Portal configuration task list | 112 |
| Configuration prerequisites | 113 |
| Specifying the local portal server for Layer 2 portal authentication | 114 |
| Configuring the local portal server | 114 |
| Customizing authentication pages | 114 |
| Configuring the local portal server | 117 |
| Enabling Layer 2 portal authentication | 118 |
| Controlling access of portal users | 119 |
| Configuring a portal-free rule | 119 |
| Setting the maximum number of online portal users | 119 |
| Specifying an authentication domain for portal users | 120 |
| Adding a web proxy server port number | 120 |
| Enabling support for portal user moving | 121 |
| Specifying the Auth-Fail VLAN for portal authentication | 122 |
| Specifying the auto redirection URL for authenticated portal users | 122 |
| Configuring portal detection functions | 123 |
| Logging off portal users | 123 |
| Displaying and maintaining portal | 123 |
| Portal configuration examples | 124 |
| Configuring Layer 2 portal authentication | 124 |
| Troubleshooting portal | 128 |
| Inconsistent keys on the access device and the portal server | 128 |
| Incorrect server port number on the access device | 128 |
| Triple authentication configuration | 130 |
| Triple authentication overview | 130 |
| Triple authentication mechanism | 130 |
| Using triple authentication with other features | 131 |
| Configuring triple authentication | 131 |
| Triple authentication configuration examples | 132 |
| Triple authentication basic function configuration example | 132 |
| Triple authentication supporting VLAN assignment and Auth-Fail VLAN configuration example | 135 |
| Port security configuration | 140 |
| Port security overview | 140 |
| Port security features | 140 |
| Port security modes | 140 |
| Support for guest VLAN and Auth-Fail VLAN | 143 |
| Port security configuration task list | 143 |
| Enabling port security | 144 |
| Configuration prerequisites | 144 |
| Configuration procedure | 144 |
| Setting the maximum number of secure MAC addresses | 144 |

| | |
|--|------------|
| Setting the port security mode | 145 |
| Configuration prerequisites | 145 |
| Configuration procedure | 145 |
| Configuring port security features | 146 |
| Configuring NTK | 146 |
| Configuring intrusion protection | 147 |
| Configuring port security traps | 147 |
| Configuring secure MAC addresses | 148 |
| Configuration prerequisites | 148 |
| Configuration procedure | 148 |
| Ignoring authorization information from the server | 149 |
| Displaying and maintaining port security | 149 |
| Port security configuration examples | 150 |
| Configuring the autoLearn mode | 150 |
| Configuring the userLoginWithOUI mode | 152 |
| Configuring the macAddressElseUserLoginSecure mode | 156 |
| Troubleshooting port security | 159 |
| Cannot set the port security mode | 159 |
| Cannot configure secure MAC addresses | 160 |
| Cannot change port security mode when a user is online | 160 |
| User profile configuration | 161 |
| User profile overview | 161 |
| User profile configuration task list | 161 |
| Creating a user profile | 161 |
| Configuration prerequisites | 161 |
| Creating a user profile | 161 |
| Configuring a user profile | 162 |
| Enabling a user profile | 162 |
| Displaying and maintaining user profile | 163 |
| Password control configuration | 164 |
| Password control overview | 164 |
| Password control configuration task list | 166 |
| Configuring password control | 167 |
| Enabling password control | 167 |
| Setting global password control parameters | 167 |
| Setting user group password control parameters | 168 |
| Setting local user password control parameters | 169 |
| Setting super password control parameters | 170 |
| Setting a local user password in interactive mode | 170 |
| Displaying and maintaining password control | 170 |
| Password control configuration example | 171 |
| HABP configuration | 174 |
| HABP overview | 174 |
| Configuring HABP | 175 |
| Configuring the HABP server | 175 |
| Configuring an HABP client | 175 |
| Displaying and maintaining HABP | 176 |
| HABP configuration example | 176 |
| Network requirements | 176 |
| Configuration procedure | 177 |
| Public key configuration | 179 |
| Asymmetric key algorithm overview | 179 |
| Basic concepts | 179 |

| | |
|---|------------|
| Key algorithm types | 179 |
| Asymmetric key algorithm applications | 179 |
| Configuring the local asymmetric key pair | 180 |
| Creating an asymmetric key pair | 180 |
| Displaying or exporting the local RSA or DSA host public key | 180 |
| Destroying an asymmetric key pair | 181 |
| Configuring a peer public key | 181 |
| Displaying and maintaining public keys | 182 |
| Public key configuration examples | 182 |
| Configuring a peer public key manually | 182 |
| Importing a peer public key from a public key file | 184 |
| PKI configuration | 187 |
| PKI overview | 187 |
| PKI terms | 187 |
| PKI architecture | 188 |
| PKI applications | 188 |
| How does PKI work | 189 |
| PKI configuration task list | 189 |
| Configuring an entity DN | 190 |
| Configuring a PKI domain | 191 |
| Submitting a PKI certificate request | 192 |
| Submitting a certificate request in auto mode | 193 |
| Submitting a certificate request in manual mode | 193 |
| Retrieving a certificate manually | 194 |
| Configuring PKI certificate verification | 195 |
| Destroying a local RSA key pair | 196 |
| Deleting a certificate | 196 |
| Configuring an access control policy | 197 |
| Displaying and maintaining PKI | 197 |
| PKI configuration examples | 198 |
| Requesting a certificate from a CA running RSA Keon | 198 |
| Requesting a certificate from a CA running Windows 2003 Server | 201 |
| Configuring a certificate attribute-based access control policy | 204 |
| Troubleshooting PKI | 206 |
| Failed to retrieve a CA certificate | 206 |
| Failed to request a local certificate | 206 |
| Failed to retrieve CRLs | 207 |
| SSH2.0 configuration | 208 |
| SSH2.0 overview | 208 |
| Introduction to SSH2.0 | 208 |
| How does SSH work | 208 |
| Configuring the device as an SSH server | 210 |
| SSH server configuration task list | 210 |
| Generating a DSA or RSA key pair | 211 |
| Enabling the SSH server function | 211 |
| Configuring the user interfaces for SSH clients | 212 |
| Configuring a client public key | 212 |
| Configuring an SSH user | 213 |
| Setting the SSH management parameters | 214 |
| Configuring the device as an SSH client | 215 |
| SSH client configuration task list | 215 |
| Specifying a source IP address/interface for the SSH client | 215 |
| Configuring whether first-time authentication is supported | 216 |
| Establishing a connection between the SSH client and server | 217 |

| | |
|---|------------|
| Displaying and maintaining SSH | 217 |
| SSH server configuration examples | 218 |
| When switch acts as server for password authentication | 218 |
| When switch acts as server for publickey authentication | 220 |
| SSH client configuration examples | 225 |
| When switch acts as client for password authentication | 225 |
| When switch acts as client for publickey authentication | 228 |
| SFTP configuration | 231 |
| SFTP overview | 231 |
| Configuring the device as an SFTP server | 231 |
| Configuration prerequisites | 231 |
| Enabling the SFTP server | 231 |
| Configuring the SFTP connection idle timeout period | 231 |
| Configuring the device an SFTP client | 232 |
| Specifying a source IP address or interface for the SFTP client | 232 |
| Establishing a connection to the SFTP server | 232 |
| Working with SFTP directories | 233 |
| Working with SFTP files | 233 |
| Displaying help information | 234 |
| Terminating the connection to the remote SFTP server | 234 |
| SFTP client configuration example | 235 |
| SFTP server configuration example | 238 |
| SSL configuration | 241 |
| SSL overview | 241 |
| SSL security mechanism | 241 |
| SSL protocol stack | 242 |
| SSL configuration task list | 242 |
| Configuring an SSL server policy | 242 |
| Configuration prerequisites | 242 |
| Configuration procedure | 243 |
| SSL server policy configuration example | 243 |
| Configuring an SSL client policy | 245 |
| Configuration prerequisites | 245 |
| Configuration procedure | 245 |
| Displaying and maintaining SSL | 246 |
| Troubleshooting SSL | 246 |
| SSL handshake failure | 246 |
| TCP attack protection configuration | 248 |
| TCP attack protection overview | 248 |
| Enabling the SYN cookie feature | 248 |
| Displaying and maintaining TCP attack protection | 248 |
| IP source guard configuration | 249 |
| IP source guard overview | 249 |
| Introduction to IP source guard | 249 |
| IP source guard binding | 249 |
| Configuring IPv4 source guard binding | 251 |
| Configuring a static IPv4 source guard binding entry | 252 |
| Configuring the dynamic IPv4 source guard binding function | 252 |
| Configuring IPv6 source guard binding | 253 |
| Configuring a static IPv6 source guard binding entry | 253 |
| Configuring the dynamic IPv6 source guard binding function | 254 |
| Displaying and maintaining IP source guard | 255 |
| IP source guard configuration examples | 256 |

| | |
|--|------------|
| Static IPv4 source guard binding entry configuration example | 256 |
| Global static binding excluded port configuration example | 257 |
| Dynamic IPv4 source guard binding by DHCP snooping configuration example | 259 |
| Dynamic IPv4 source guard binding by DHCP relay configuration example | 260 |
| Static IPv6 source guard binding entry configuration example | 261 |
| Dynamic IPv6 source guard binding by DHCPv6 snooping configuration example | 262 |
| Dynamic IPv6 source guard binding by ND snooping configuration example | 263 |
| Troubleshooting IP source guard | 264 |
| Neither static binding entries nor the dynamic binding function can be configured | 264 |
| ARP attack protection configuration | 265 |
| ARP attack protection overview | 265 |
| ARP attack protection configuration task list | 265 |
| Configuring ARP defense against IP packet attacks | 266 |
| Introduction | 266 |
| Configuring ARP source suppression | 266 |
| Enabling ARP black hole routing | 267 |
| Displaying and maintaining ARP defense against IP packet attacks | 267 |
| Configuring ARP packet rate limit | 267 |
| Introduction | 267 |
| Configuring ARP packet rate limit | 267 |
| Configuring source MAC address based ARP attack detection | 268 |
| Introduction | 268 |
| Configuration procedure | 268 |
| Displaying and maintaining source MAC address based ARP attack detection | 269 |
| Configuring ARP packet source MAC address consistency check | 269 |
| Introduction | 269 |
| Configuration procedure | 269 |
| Configuring ARP active acknowledgement | 270 |
| Introduction | 270 |
| Configuration procedure | 270 |
| Configuring ARP detection | 270 |
| Introduction | 270 |
| Enabling ARP detection based on static IP source guard binding Entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses | 271 |
| Configuring ARP detection based on specified objects | 272 |
| Configuring ARP restricted forwarding | 273 |
| Displaying and maintaining ARP detection | 273 |
| ARP detection configuration example I | 273 |
| ARP detection configuration example II | 275 |
| ARP restricted forwarding configuration example | 276 |
| Configuring ARP automatic scanning and fixed ARP | 278 |
| Introduction | 278 |
| Configuration procedure | 278 |
| Configuring ARP gateway protection | 279 |
| Introduction | 279 |
| Configuration procedure | 279 |
| ARP gateway protection configuration example | 280 |
| Configuring ARP filtering | 280 |
| Introduction | 280 |
| Configuration procedure | 281 |
| ARP filtering configuration example | 281 |
| ND attack defense configuration | 283 |
| Introduction to ND attack defense | 283 |
| Enabling source MAC consistency check for ND packets | 284 |

| | |
|---|------------|
| Configuring the ND detection function | 284 |
| Introduction to ND detection | 284 |
| Configuring ND detection | 285 |
| Displaying and maintaining ND detection | 285 |
| ND detection configuration example | 286 |
| Support and other resources | 288 |
| Contacting HP | 288 |
| Subscription service | 288 |
| Related information | 288 |
| Documents | 288 |
| Websites | 288 |
| Conventions | 289 |
| Index | 291 |

AAA configuration

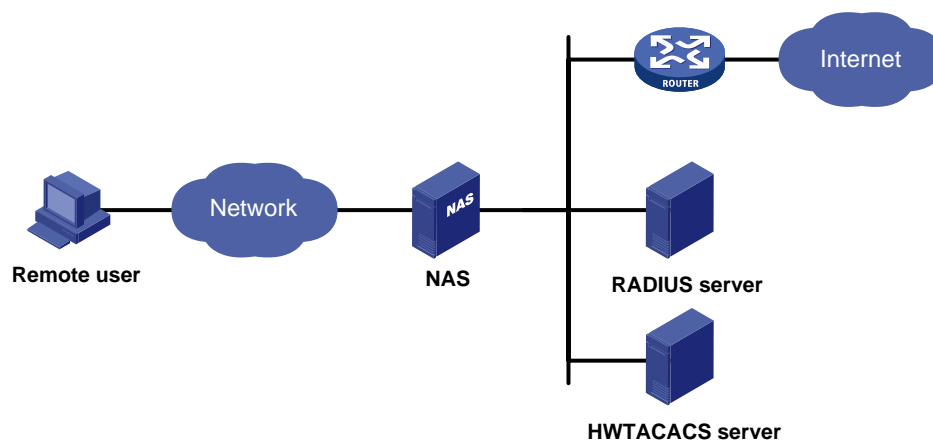
AAA overview

Authentication, Authorization, and Accounting (AAA) provides a uniform framework for implementing network access management. It provides 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 device can be granted read and print permissions to the files on the device.
- 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) and the server maintains user information centrally. In an AAA network, a NAS is a server for users but a client for the AAA servers, as shown in [Figure 1](#).

Figure 1 Network diagram for AAA



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 required. For example, if your company only wants employees to be authenticated before they access specific resources, you only need to 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 device supports using RADIUS and HWTACACS for AAA. 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. RADIUS 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, for example, Ethernet and ADSL. RADIUS provides access authentication and authorization services, and its accounting function collects and records network resource usage information.

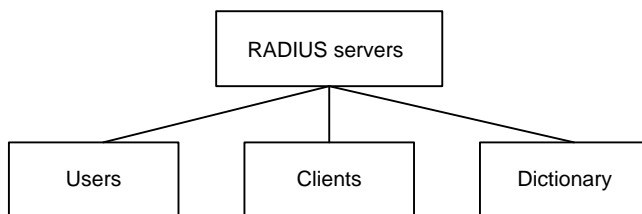
Client/server model

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

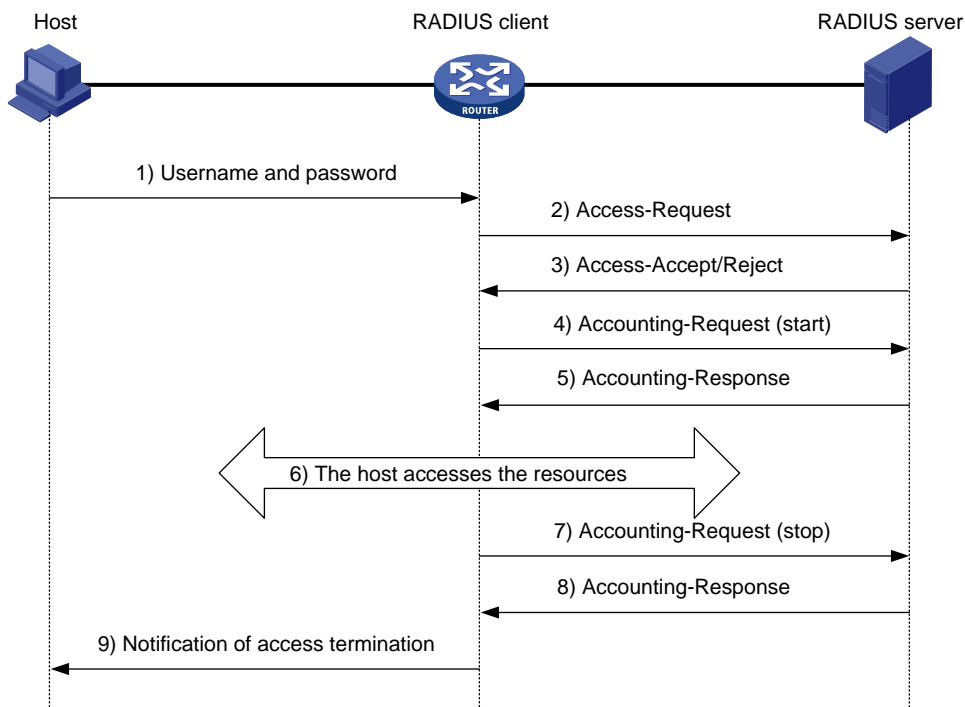
Information exchanged between a RADIUS client and the RADIUS server is authenticated with a shared key, which is never transmitted over the network. This enhances information exchange security. In addition, to prevent user passwords from being intercepted in non-secure networks, RADIUS encrypts passwords before transmitting them.

A RADIUS server supports multiple user authentication methods, such as the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP). Moreover, a RADIUS server can act as the client of another AAA server to provide authentication proxy services.

RADIUS basic message exchange process

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

Figure 3 RADIUS basic message exchange process



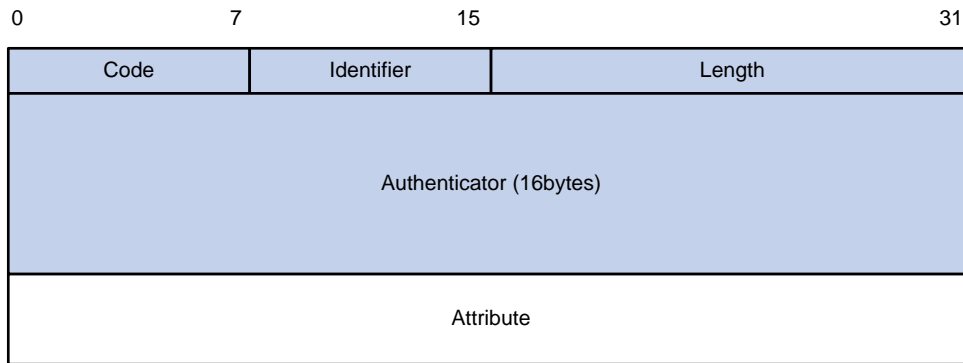
RADIUS operates in the following manner:

1. The host initiates a connection request carrying the 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, it sends back an Access-Accept message containing the user's authorization information. If the authentication fails, it 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.
9. The user stops access to network resources.

RADIUS packet format

RADIUS uses UDP to transmit messages. It ensures smooth message exchange between the RADIUS server and the client through 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:

1. The Code field (1 byte long) indicates the type of the RADIUS packet.

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 correctly recorded the accounting information. |

2. The Identifier field (1 byte long) is used to match request and response packets and to detect retransmitted request packets. Request and response packets of the same type have the same identifier.
3. 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 neglected upon reception. 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 20 to 4096.
4. 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.

5. The Attribute field, with a variable length, carries the specific authentication, authorization, and accounting information that defines the configuration details of the request or response. This field contains multiple attributes, and each attribute is represented in triplets of Type, Length, and Value.
 - Type (1 byte long)—Indicates the type of the attribute. It is in the range 1 to 255. See [Table 2](#) for commonly used attributes for RADIUS authentication, authorization and accounting, which are defined in RFC 2865, RFC 2866, RFC 2867, and RFC 2868. For more information about commonly used standard RADIUS attributes, see “[Commonly used standard RADIUS attributes.](#)”
 - Length (1 byte long)—Indicates the 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 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 |

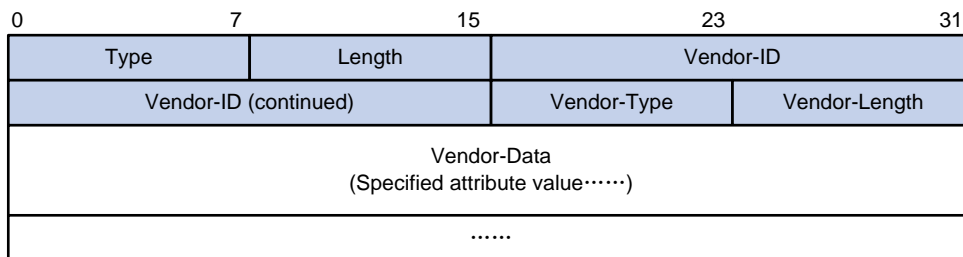
Extended RADIUS attributes

The RADIUS protocol features excellent extensibility. Attribute 26 (Vendor-Specific) 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 type-length-value (TLV) sub-attributes in RADIUS packets for extension in applications. As shown in [Figure 5](#), a sub-attribute that can be encapsulated in Attribute 26 consists of the following parts:

- Vendor-ID (4 bytes long)—Indicates the ID of the vendor. Its most significant byte is 0; 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 mainly provides AAA services for Point-to-Point Protocol (PPP) users, Virtual Private Dial-up Network (VPDN) users, and terminal users. In a typical HWTACACS application, some terminal users need to log in to the NAS for operations. Working as the HWTACACS client, the NAS sends the username and password of a user to the HWTACACS sever for authentication. After passing authentication and being authorized, the user logs in to the device and performs operations, and the HWTACACS server records the operations that the user performs.

Differences between HWTACACS and RADIUS

HWTACACS and RADIUS both provide authentication, authorization, and accounting services. They have many features in common, like using a client/server model, using shared keys for user information security, and providing flexibility and extensibility. [Table 3 lists their differences.](#)

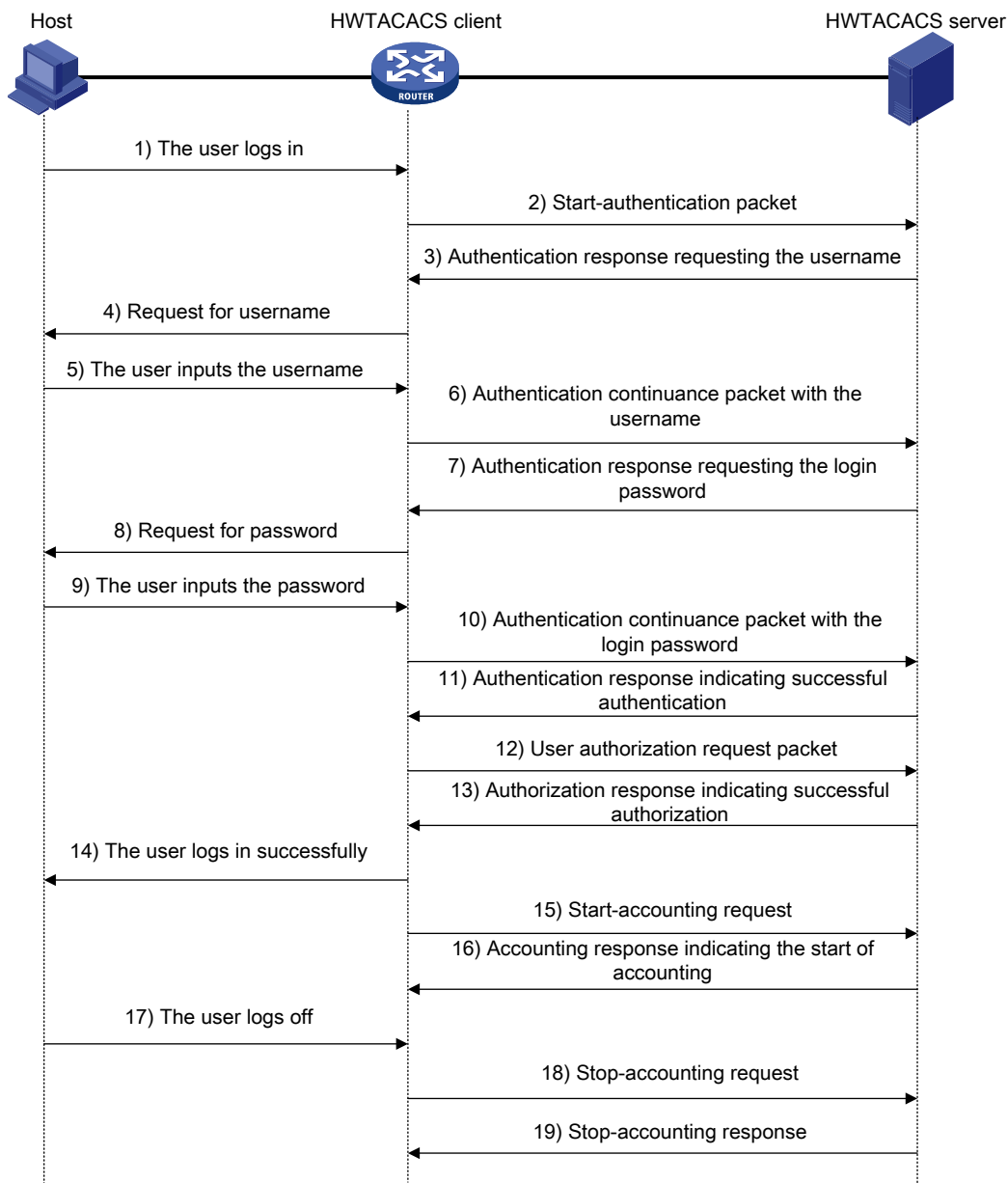
Table 3 Primary differences between HWTACACS and RADIUS

| 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 AAA authorization. A user can use only commands that are not only of, or lower than, the user level but also authorized by the HWTACACS server. | Does not support authorization of configuration commands. Which commands a user can use depends on the level of the user and a user can use all the commands of, or lower than, the user level. |

HWTACACS basic message exchange process

The following takes a Telnet user as an example to describe how HWTACACS performs user authentication, authorization, and accounting.

Figure 6 HWTACACS basic message exchange process for a Telnet user



Here is the process:

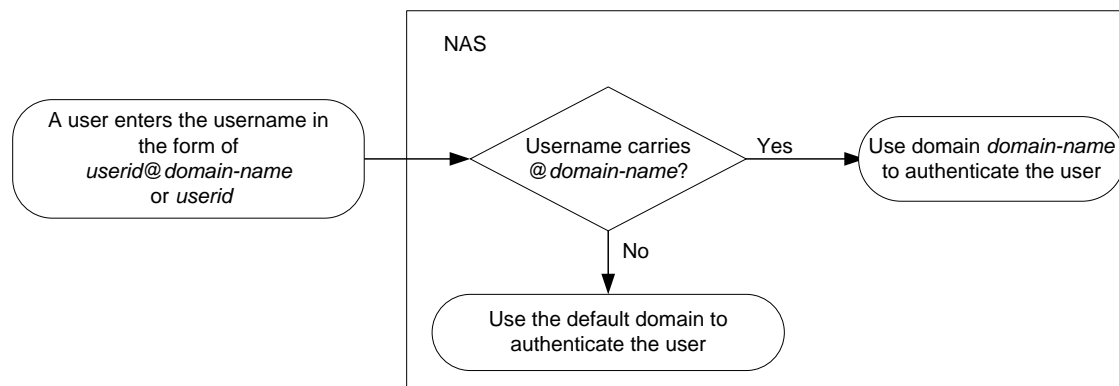
1. A Telnet user sends an access request to the HWTACACS client.
2. Upon receiving the request, the HWTACACS client sends a start-authentication packet to the HWTACACS server.
3. The HWTACACS server sends back an authentication response to request the username.
4. Upon receiving the response, the HWTACACS client asks the user for the username.
5. The user inputs the username.
6. After receiving the username, 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 inputs 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 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 Determine the ISP domain of a user by the username



The authentication, authorization, and accounting of a user depends on the AAA methods configured for the domain that the user belongs to. 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.

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

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

For a user who has logged in to the device, AAA provides the following services to enhance device 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, ensuring that login users execute only commands they are authorized to execute. For more information about command authorization, see the *Fundamentals Configuration Guide*.
- Command accounting—Allows the accounting server to record all commands executed on the device or all authorized commands successfully executed. For more information about command accounting, see the *Fundamentals Configuration Guide*.
- Level switching authentication—Allows the authentication server to authenticate users performing 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 the *Fundamentals Configuration Guide*.

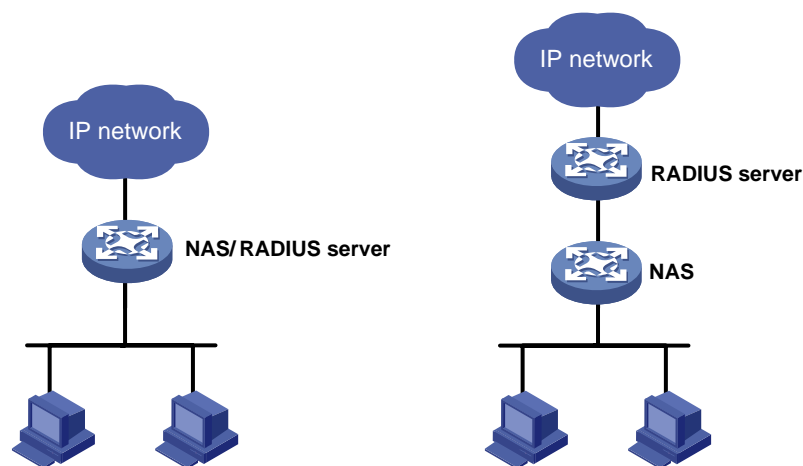
You can configure different authentication, authorization, and accounting methods for different users in a domain. See “[Configuring AAA methods for ISP domains](#).”

RADIUS server feature of the device

Generally, the RADIUS server runs on a computer or workstation, and the RADIUS client runs on a NAS device. 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 device or different devices.

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



A network device serving as the RADIUS server can provide the following functions:

- User information management—Supports creating, modifying, and deleting user information, including the username, password, authority, lifetime, and user description.
- RADIUS client information management—Supports creating, and deleting RADIUS clients, which are identified by IP addresses and configured with attributes such as a shared key. After being configured with a managed client range, 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. RADIUS accounting is not supported.

Upon receiving a RADIUS packet, a device working as the RADIUS server checks whether the sending client 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:

The UDP port number for RADIUS authentication is 1812 in the standard RADIUS protocol, but is 1645 on HP devices. Specify 1645 as the authentication port number when you use an HP device as a RADIUS client.

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. |
| 8 | Framed-IP-Address | IP address to be configured for the user. |
| 11 | Filter-ID | Name of the filter list. |

| No. | Attribute | Description |
|-----|--------------------|---|
| 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. With 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 1—RADIUS • 2—Local • 3—Remote |
| 60 | CHAP-Challenge | CHAP challenge generated by the NAS for MD5 calculation during CHAP authentication. |
| 61 | NAS-Port-Type | Type of the physical port of the NAS that is authenticating the user. Possible values are as follows: <ul style="list-style-type: none"> • 15—Ethernet • 16—Any type of ADSL • 17—Cable (with cable for cable TV) • 201—VLAN • 202—ATM <p>If the port is an ATM or Ethernet one and VLANs are implemented on it, the value of this attribute is 201.</p> |
| 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. |

| No. | Attribute | Description |
|-----|-----------------------|---|
| 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 | <p>Operation for the session, used for session control. Possible values are as follows:</p> <ul style="list-style-type: none"> • 1—Trigger-Request • 2—Terminate-Request • 3—SetPolicy • 4—Result • 5—PortalClear |
| 24 | Control_Identifier | <p>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.</p> <p>For Accounting-Request packets of the start, stop, and interim update types, the Control-Identifier attribute, if present, makes no sense.</p> |
| 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 | <p>Working directory of the FTP user.</p> <p>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.</p> |
| 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 | IP address and MAC address of the user 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 that needs to be sent from the server to the client transparently |

| No. | Sub-attribute | Description |
|-----|---------------------------|---|
| 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 |

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, and 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

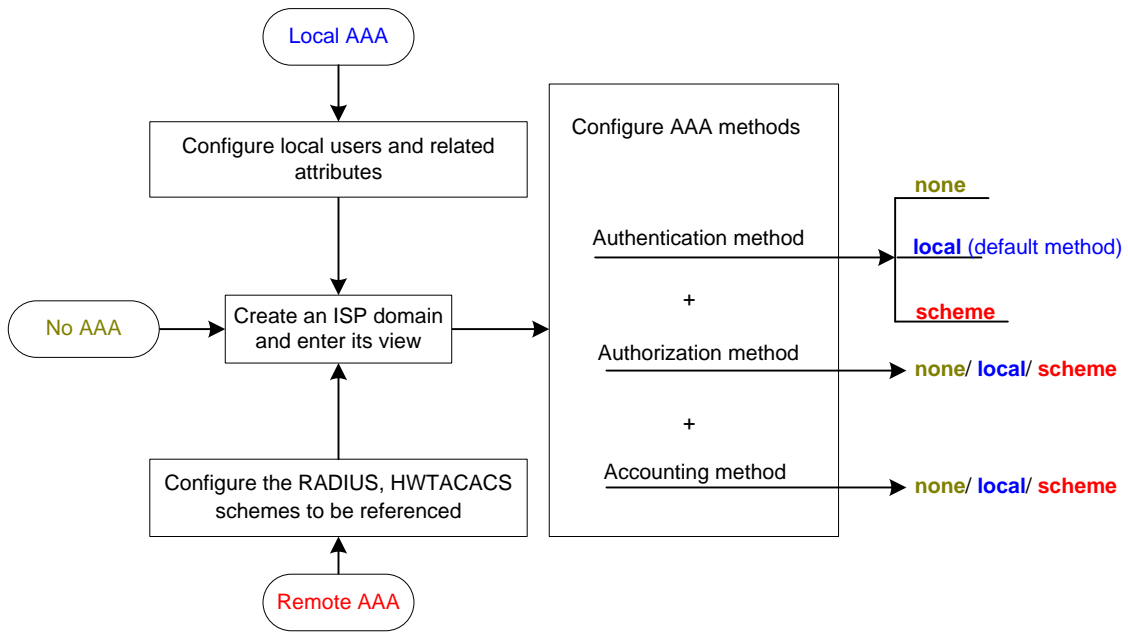


Table 4 AAA configuration task list

| Task | Remarks | |
|---|--|---|
| Configuring AAA schemes | Configuring local users | Required |
| | Configuring RADIUS schemes | Complete at least one task. |
| | 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 | |
| Tearing down user connections forcibly | Optional | |
| Configuring a network device as a RADIUS server | Optional | |
| Displaying and maintaining AAA | Optional | |

NOTE:

For login users, you must configure the login authentication mode for the user interfaces as **scheme** before performing the above configurations. For more information, see the *Fundamentals Configuration Guide*.

Configuring AAA schemes

Configuring local users

For local authentication, you must create local users and configure user attributes on the device in advance. The local users and attributes are stored in the local user database on the device. 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, and Terminal.

- User state

Indicates whether or not a local user can request network services. There are two user states: active and blocked. A user in the active state can request network services, but a user in the 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.

- Expiration time

Indicates the expiration time of a local user account. A user must use a local user account that has not expired to pass local authentication.

- 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 improve 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 the chapter [“Password control configuration.”](#)

- Binding attributes

Binding attributes are used to control the scope of users. Binding attributes are checked during authentication. If the attributes of a user do not match the binding attributes configured for the user on the access device, 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.”](#)

- Authorization attributes

Authorization attributes indicate the rights that a user has after passing local authentication. Authorization attributes include the ACL, PPP callback number, 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.”](#)

You can configure an authorization attribute in user group view or local user view, making 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 steps to configure attributes for a local user:

| To do... | Use the command... | Remarks |
|--|---|--|
| Enter system view | system-view | — |
| Set the password display mode for all local users | local-user password-display-mode { auto cipher-force } | Optional auto by default, indicating to display the password of a local user in the way indicated by the password command. |
| Add a local user and enter local user view | local-user <i>user-name</i> | Required No local user exists by default. |
| Configure a password for the local user | password { cipher simple } <i>password</i> | Optional |
| Place the local user to the state of active or blocked | state { active block } | Optional When created, a local user is in the active state by default, and the user can request network services. |
| Set the maximum number of users using the local user account | access-limit <i>max-user-number</i> | Optional By default, there is no limit on the maximum number of users that use the same local user account. This limit is not effective for FTP users. |
| Configure the password control attributes for the local user | Set the password aging time password-control aging <i>aging-time</i> | Optional By default, the setting for the user group is used. If there is no such setting for the user group, the global setting is used. |
| | Set the minimum password length password-control length <i>length</i> | Optional By default, the setting for the user group is used. If there is no such setting for the user group, the global setting is used. |

| To do... | Use the command... | Remarks |
|---|--|--|
| Configure the password composition policy | password-control composition type-number <i>type-number</i> [type-length <i>type-length</i>] | Optional By default, the setting for the user group is used. If there is no such setting for the user group, the global setting is used. |
| Specify the service types for the local user | service-type { ftp lan-access { ssh telnet terminal } * portal } | Required By default, no service is authorized to a local user. |
| Configure the binding attributes for the local user | bind-attribute { call-number <i>call-number</i> [<i>: subcall-number</i>] ip <i>ip-address</i> location port slot- <i>number subslot-number port-</i> <i>number</i> mac <i>mac-address</i> vlan <i>vlan-id</i> } * | Optional By default, no binding attribute is configured for a local user. ip , location , mac , and vlan are supported for LAN users. No binding attribute is supported for other types of local users. |
| Configure the authorization attributes for the local user | authorization-attribute { acl <i>acl-</i> <i>number</i> callback-number <i>callback-number</i> idle-cut <i>minute</i> level <i>level</i> user- profile <i>profile-name</i> user-role security-audit vlan <i>vlan-id</i> work-directory <i>directory-name</i> } * | 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 and terminal 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. |
| Set the expiration time of the local user | expiration-date <i>time</i> | Optional Not set by default When some users need to access the network temporarily, create a guest account and specify an expiration time for the account. |
| Assign the local user to a user group | group <i>group-name</i> | Optional By default, a local user belongs to the default user group system . |

NOTE:

- For more information about password control attribute commands, see the chapter “Password control configuration.”
 - On a device supporting the password control feature, local user passwords are not displayed, and the **local-user password-display-mode** command is not effective.
 - With the **local-user password-display-mode cipher-force** command configured, a local user password is always displayed in cipher text, regardless of the configuration of the **password** command. In this case, if you use the **save** command to save the configuration, all existing local user passwords will still be displayed in cipher text after the device restarts, even if you restore the display mode to **auto**.
 - The **access-limit** command configured for a local user takes effect only when local accounting is configured.
 - 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 the *Fundamentals Configuration Guide*.
 - Be cautious when deciding which binding attributes should be configured for a local user. Binding attributes are checked upon local authentication of a user. If the checking fails, the user fails the authentication.
 - Every configurable authorization attribute has its definite application environments and purposes. When configuring authorization attributes for a local user, consider what attributes are needed.
-

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.

Follow these steps to configure attributes for a user group:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Create a user group and enter user group view | user-group <i>group-name</i> | Required |
| Configure password control attributes for the user group | Set the password aging time | password-control aging <i>aging-time</i> Optional By default, the global setting is used. |
| | Set the minimum password length | password-control length <i>length</i> Optional By default, the global setting is used. |
| | Configure the password composition policy | password-control composition type-number <i>type-number</i> [type-length <i>type-length</i>] Optional By default, the global setting is used. |

| To do... | Use the command... | Remarks |
|---|--|--|
| Configure the authorization attributes for the user group | authorization-attribute { acl <i>acl-number</i> callback-number <i>callback-number</i> idle-cut <i>minute</i> level <i>level</i> user-profile <i>profile-name</i> vlan <i>vlan-id</i> work-directory <i>directory-name</i> } * | Optional By default, no authorization attribute is configured for a user group. |

Displaying and maintaining local users and local user groups

| To do... | Use the command... | Remarks |
|--|---|-----------------------|
| Display local user information | display local-user [idle-cut { disable enable } service-type { ftp lan-access portal ssh telnet terminal } state { active block } user-name <i>user-name</i> vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |
| Display the user group configuration information | display user-group [<i>group-name</i>] [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |

Configuring RADIUS schemes

A RADIUS scheme specifies the RADIUS servers that the device can cooperate with and defines a set of parameters that the device 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 mainly 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 relevant parameters | Optional |
| Setting the shared keys for RADIUS packets | Optional |
| Setting the maximum number of RADIUS request transmission attempts | Optional |
| Setting the supported RADIUS server type | Optional |
| Setting the status of RADIUS servers | Optional |
| Setting the username format and traffic statistics units | Optional |
| Specifying a source IP address for outgoing RADIUS packets | Optional |
| Setting timers for controlling communication with RADIUS servers | Optional |

| Task | Remarks |
|--|----------|
| Configuring RADIUS accounting-on | Optional |
| Specifying a security policy server | Optional |
| Configuring interpretation of RADIUS class attribute as CAR parameters | Optional |
| Enabling the RADIUS trap function | Optional |
| Enabling the listening port of the RADIUS client | 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:

| To do... | Use the command... | Remarks |
|---|--|---|
| Enter system view | system-view | — |
| Create a RADIUS scheme and enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | Required No RADIUS scheme by default |

NOTE:

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

Specifying the RADIUS authentication/authorization servers

Follow these steps to specify the RADIUS authentication/authorization servers:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Specify the primary RADIUS authentication/authorization server | primary authentication { <i>ip-address</i> [<i>port-number</i> key string] * ipv6 <i>ipv6-address</i> [<i>port-number</i> key string] * } | Required Configure at least one command. |
| Specify the secondary RADIUS authentication/authorization server | secondary authentication { <i>ip-address</i> [<i>port-number</i> key string] * ipv6 <i>ipv6-address</i> [<i>port-number</i> key string] * } | No authentication/authorization server is specified by default. |

NOTE:

- If both the primary and secondary authentication/authorization servers are specified, the secondary one is used when the primary one is not reachable.
 - If redundancy is not required, specify only the primary RADIUS authentication/authorization server.
 - In practice, you may specify one RADIUS server as the primary authentication/authorization server, and up to 16 RADIUS servers as the secondary authentication/authorization servers, or specify a server as the primary authentication/authorization server for a scheme and as the secondary authentication/authorization servers for another scheme at the same time.
 - The IP addresses of the primary and secondary authentication/authorization servers for a scheme must be different from each other. Otherwise, the configuration will fail.
 - All servers for authentication/authorization and accountings, primary or secondary, must use IP addresses of the same IP version.
-

Specifying the RADIUS accounting servers and 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, if any. 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 device disconnect users for whom no accounting response is received before the number of accounting attempts reaches the limit.

When the device 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 device 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 device discards the packet.

Follow these steps to specify the RADIUS accounting servers and perform related configurations:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Specify the primary RADIUS accounting server | primary accounting { <i>ip-address</i> [<i>port-number</i> <i>key string</i>] * ipv6 <i>ipv6-address</i> [<i>port-number</i> <i>key string</i>] * } | Required Configure at least one command. |
| Specify the secondary RADIUS accounting server | secondary accounting { <i>ip-address</i> [<i>port-number</i> <i>key string</i>] * ipv6 <i>ipv6-address</i> [<i>port-number</i> <i>key string</i>] * } | No accounting server is specified by default. |
| Enable the device to buffer stop-accounting requests to which no responses are received | stop-accounting-buffer enable | Optional Enabled by default |
| Set the maximum number of stop-accounting attempts | retry stop-accounting <i>retry-times</i> | Optional 500 by default |
| Set the maximum number of real-time accounting attempts | retry realtime-accounting <i>retry-times</i> | Optional 5 by default |

NOTE:

- 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 serving users, the device 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.
-

Setting the shared keys for RADIUS packets

The RADIUS client and RADIUS server use the MD5 algorithm to encrypt packets exchanged between them and use shared keys to verify the packets. They must use the same shared key for the same type of packets.

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.

Follow these steps to set the shared keys for RADIUS packets:

| To do... | Use the command... | Remarks |
|--|--|--------------------------------------|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Set the shared key for RADIUS authentication/authorization or accounting packets | key { accounting authentication } <i>string</i> | Required No shared key by default |

NOTE:

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

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 reliability. If a NAS sends a RADIUS request to a RADIUS server but receives no response before the response timeout timer 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 the active state. If no other servers are in the active state at the time, it considers the authentication a failure. For more information about RADIUS server states, see “[Setting the status of RADIUS servers.](#)”

Follow these steps to set the maximum number of RADIUS request transmission attempts:

| To do... | Use the command... | Remarks |
|--|--|--------------------------|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Set the maximum number of RADIUS request transmission attempts | retry <i>retry-times</i> | Optional 3 by default |

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 supported RADIUS server type

The supported RADIUS server type determines the type of the RADIUS protocol that the device 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 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 device to function as a RADIUS server to authenticate login users, you must set the RADIUS server type to **standard**.

Follow these steps to set the RADIUS server type:

| To do... | Use the command... | Remarks |
|----------------------------|--|--|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Set the RADIUS server type | server-type { extended standard } | Optional standard by default |

NOTE:

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

Setting the status of RADIUS servers

By setting the status of RADIUS servers to blocked or active, you can control which servers the device will communicate with for authentication, authorization, and accounting or turn to when the current servers are not available anymore. In practice, you can specify one primary RADIUS server and multiple secondary RADIUS servers, with the secondary ones as the backup of the primary one. Generally, the device chooses servers based on these rules:

- When the primary server is in the active state, the device communicates with the primary server. If the primary server fails, the device changes the state of the primary server to blocked and starts a quiet timer for the server, and then turns to a secondary server in the active state (a secondary server configured earlier has a higher priority). If the secondary server is unreachable, the device changes the server's status to blocked, starts a quiet timer for the server, and continues to check the next secondary server in the active state. This search process continues until the device finds an available secondary server or has checked all secondary servers in the active state. If the quiet timer of a server expires or an authentication or accounting response is received from the server, the state of the server changes back to active automatically, but the device does not check the server again. If no server is found reachable during one search process, the device considers the authentication or accounting attempt a failure.
- Once the accounting process of a user starts, the device 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 of the user cannot be delivered to the server anymore.

- If you remove an authentication or accounting server in use, the communication of the device with the server will soon time out, and the device will look for a server in the active state from scratch: it checks the primary server (if any) first and then the secondary servers in the order they are configured.
- When the primary server and secondary servers are all in the blocked state, the device communicates with the primary server. If the primary server is available, its state changes to active; otherwise, its state remains to be blocked.
- If one server is in the active state and the others are in the blocked state, the device only tries to communicate with the server in the active state, even if the server is unavailable.
- After receiving an authentication/accounting response from a server, the device changes the state of the server identified by the source IP address of the response to active if the current state of the server is blocked.

By default, the device sets the status of all RADIUS servers to active. In some cases, however, you may need to change the status of a server. For example, if a server fails, you can change the status of the server to blocked to avoid communication with the server.

Follow these steps to set the status of RADIUS servers:

| To do... | Use the command... | Remarks |
|--|--|--|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| 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 } | Optional |
| Set the status of the secondary RADIUS authentication/authorization server | state secondary authentication [ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i>] { active block } | active for every server specified in the RADIUS scheme by default |
| Set the status of the secondary RADIUS accounting server | state secondary accounting [ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i>] { active block } | |

NOTE:

- The server status set by the **state** command cannot be saved in the configuration file and will be restored to active every time the server restarts.
- To display the states of the servers, use the **display radius scheme** command.

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 device 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 device must remove the domain name of each username before sending the username. You can set the username format on the device for this purpose.

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

Follow these steps to set the username format and the traffic statistics units for a RADIUS scheme:

| To do... | Use the command... | Remarks |
|---|--|---|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| 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 the username. |
| 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 byte for data flows and one-packet for data packets by default. |

NOTE:

- 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 will be 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 ensure that usernames sent to the RADIUS server carry no ISP domain name.

Specifying a 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.

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 this order:

1. The source IP address specified for the RADIUS scheme.
2. The source IP address specified in system view.
3. The IP address of the outbound interface specified by the route.

Follow these steps to specify a source IP address for all RADIUS schemes:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Specify a source IP address for outgoing RADIUS packets | radius nas-ip { <i>ip-address</i> ipv6 <i>ipv6-address</i> } | Required By default, the IP address of the outbound interface is used as the source IP address. |

Follow these steps to specify a source IP address for a specific RADIUS scheme:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Specify a source IP address for outgoing RADIUS packets | nas-ip { <i>ip-address</i> ipv6 <i>ipv6-address</i> } | Required 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 device 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 device starts this timer. If the device 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 the blocked state. If a server is not reachable, the device changes the server's status to blocked, starts this timer for the server, and tries to communicate with another server in the active state. After this timer expires, the device changes the status of the server back to active.
- Real-time accounting timer (**realtime-accounting**)—Defines the interval at which the device sends real-time accounting packets to the RADIUS accounting server for online users. To implement real-time accounting, the device must periodically send real-time accounting packets to the accounting server for online users.

Follow these steps to set timers for controlling communication with RADIUS servers:

| To do... | Use the command... | Remarks |
|--|---|-----------------------------------|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Set the RADIUS server response timeout timer | timer response-timeout <i>seconds</i> | Optional 3 seconds by default |
| Set the quiet timer for the servers | timer quiet <i>minutes</i> | Optional 5 minutes by default |
| Set the real-time accounting timer | timer realtime-accounting <i>minutes</i> | Optional 12 minutes by default |

NOTE:

- For an access module, 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, because the client connection timeout time for voice access is 10 seconds, the product of the two parameters must be less than 10 seconds; because the client connection timeout time for Telnet access is 30 seconds, the product of the two parameters must be less than 30 seconds.
 - When configuring 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 device 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 device 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 device has to repeatedly attempt to communicate with a server that is in the active state but is unreachable.
 - For more information about the maximum number of RADIUS packet retransmission attempts, see [“Setting the maximum number of RADIUS request transmission attempts.”](#)
-

Configuring RADIUS accounting-on

The accounting-on feature enables a device to send accounting-on packets to the RADIUS server after it reboots, making the server log out users who logged in through the device 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 device 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.

Follow these steps to configure the accounting-on feature for a RADIUS scheme:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Enable accounting-on and configure parameters | accounting-on enable [interval <i>seconds</i> send <i>send-times</i>] * | Required Disabled by default. The default interval is 3 seconds and the default number of send-times is 5. |

NOTE:

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

Specifying a security policy server

The core of the EAD solution is integration and cooperation, and the security policy server is the management and control center. As 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 iMC security policy server and that of the iMC configuration platform on the NAS.

Follow these steps to specify a security policy server:

| To do... | Use the command... | Remarks |
|----------------------------------|---|---|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Specify a security policy server | security-policy-server <i>ip-address</i> | Required No security policy server is specified by default |

NOTE:

You can specify up to eight security policy servers for a RADIUS scheme.

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 access devices need to interpret the attribute to implement user-based traffic monitoring and controlling. To support such applications, configure the access devices to interpret the class attribute as the CAR parameters.

Follow these steps to configure the RADIUS client to interpret the class attribute as the CAR parameters:

| To do... | Use the command... | Remarks |
|--|--|---|
| Enter system view | system-view | — |
| Enter RADIUS scheme view | radius scheme <i>radius-scheme-name</i> | — |
| Specify to interpret the class attribute as the CAR parameters | attribute 25 car | Required By default, RADIUS attribute 25 is not interpreted as CAR parameters. |

NOTE:

Whether to configure this feature depends on the implementation of the device and the RADIUS server.

Enabling the RADIUS trap function

With the RADIUS trap function, a NAS sends a trap message in either of these situations:

- The status of a RADIUS server changes. If a NAS sends and retransmits an accounting or authentication request to a RADIUS server but gets no response before the maximum number of transmission attempts is reached, it considers the server unavailable and sends a trap message. If the NAS receives a response from a RADIUS server in the blocked state, the NAS considers that the RADIUS server is reachable again and also 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 you see a trap message triggered due to a higher failure ratio, check the configurations on the NAS and the RADIUS server and the communications between them.

Follow these steps to enable the RADIUS trap function:

| To do... | Use the command... | Remarks |
|---------------------------------|---|---------------------------------|
| Enter system view | system-view | — |
| Enable the RADIUS trap function | radius trap { accounting-server-down authentication-error-threshold authentication-server-down } | Required Disabled by default |

Enabling the listening port of the RADIUS client

Follow these steps to enable the listening port of the RADIUS client:

| To do... | Use the command... | Remarks |
|--|-----------------------------|--------------------------------|
| Enter system view | system-view | — |
| Enable the listening port of the RADIUS client | radius client enable | Optional Enabled by default |

Displaying and maintaining RADIUS

| To do... | Use the command... | Remarks |
|---|---|------------------------|
| Display the configuration information of RADIUS schemes | display radius scheme [<i>radius-scheme-name</i>] [<i>slot slot-number</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display statistics about RADIUS packets | display radius statistics [<i>slot slot-number</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display information about buffered stop-accounting requests that get no responses | display stop-accounting-buffer { radius-scheme radius-server-name session-id session-id time-range start-time stop-time user-name user-name } [<i>slot slot-number</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Clear RADIUS statistics | reset radius statistics [<i>slot slot-number</i>] | Available in user view |
| Clear buffered stop-accounting requests that get no responses | reset stop-accounting-buffer { radius-scheme radius-server-name session-id session-id time-range start-time stop-time user-name user-name } [<i>slot slot-number</i>] | 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 | Optional |
| Setting the shared keys for HWTACACS packets | 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:

| To do... | Use the command... | Remarks |
|--|--|------------------------------------|
| Enter system view | system-view | — |
| Create an HWTACACS scheme and enter HWTACACS scheme view | hwtacacs scheme <i>hwtacacs-scheme-name</i> | Required 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

Follow these steps to specify the HWTACACS authentication servers:

| To do... | Use the command... | Remarks |
|--|--|---|
| Enter system view | system-view | — |
| Enter HWTACACS scheme view | hwtacacs scheme <i>hwtacacs-scheme-name</i> | — |
| Specify the primary HWTACACS authentication server | primary authentication <i>ip-address</i> [<i>port-number</i>] | Required Configure at least one command. |
| Specify the secondary HWTACACS authentication server | secondary authentication <i>ip-address</i> [<i>port-number</i>] | No authentication server is specified by default. |

NOTE:

- If both the primary and secondary authentication servers are specified, the secondary one is used when the primary one is not reachable.
 - If redundancy is not required, specify only the primary HWTACACS authentication server.
 - 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.
-

Specifying the HWTACACS authorization servers

Follow these steps to specify the HWTACACS authorization servers:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Enter HWTACACS scheme view | hwtacacs scheme <i>hwtacacs-scheme-name</i> | — |
| Specify the primary HWTACACS authorization server | primary authorization <i>ip-address</i> [<i>port-number</i>] | Required Configure at least one command. |
| Specify the secondary HWTACACS authorization server | secondary authorization <i>ip-address</i> [<i>port-number</i>] | No authorization server is specified by default. |

NOTE:

- If both the primary and secondary authorization servers are specified, the secondary one is used when the primary one is not reachable.
 - If redundancy is not required, specify only the primary HWTACACS authorization server.
 - 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.
-

Specifying the HWTACACS accounting servers

Follow these steps to specify the HWTACACS accounting servers and perform related configurations:

| To do... | Use the command... | Remarks |
|--|--|---|
| Enter system view | system-view | — |
| Enter HWTACACS scheme view | hwtacacs scheme <i>hwtacacs-scheme-name</i> | — |
| Specify the primary HWTACACS accounting server | primary accounting <i>ip-address</i> [<i>port-number</i>] | Required Configure at least one command. |
| Specify the secondary HWTACACS accounting server | secondary accounting <i>ip-address</i> [<i>port-number</i>] | No accounting server is specified by default. |

| To do... | Use the command... | Remarks |
|---|---|--------------------------------|
| Enable the device to buffer stop-accounting requests getting no responses | stop-accounting-buffer enable | Optional Enabled by default |
| Set the maximum number of stop-accounting request transmission attempts | retry stop-accounting <i>retry-times</i> | Optional 100 by default |

NOTE:

- If both the primary and secondary accounting servers are specified, the secondary server is used when the primary server is not reachable.
- If redundancy is not required, specify only the primary HWTACACS accounting server.
- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration will fail.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.
- HWTACACS does not support keeping accounts on FTP users.

Setting the shared keys for HWTACACS packets

The HWTACACS client and HWTACACS server use the MD5 algorithm to encrypt packets exchanged between them and use shared keys to verify the packets. Only when they use the same key for an exchanged packet can they receive the packets and make responses properly.

Follow these steps to set the shared keys for HWTACACS packets:

| To do... | Use the command... | Remarks |
|--|---|--------------------------------------|
| Enter system view | system-view | — |
| Enter HWTACACS scheme view | hwtacacs scheme <i>hwtacacs-scheme-name</i> | — |
| Set the shared keys for HWTACACS authentication, authorization, and accounting packets | key { accounting authentication authorization } string | Required No shared key by default |

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 device 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 device must remove the domain name of each username before sending the username. You can set the username format on the device for this purpose.

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

Follow these steps to set the username format and the traffic statistics units for an HWTACACS scheme:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|---|--|---|
| Enter HWTACACS scheme view | hwtacacs scheme <i>hwtacacs-scheme-name</i> | — |
| Set the format of 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 the username. |
| 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 byte for data flows and one-packet for data packets by default. |

NOTE:

- If an HWTACACS server does not support a username with the domain name, configure the device 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 ensure that usernames sent to the HWTACACS server carry no ISP domain name.

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.

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 this order:

1. The source IP address specified for the HWTACACS scheme.
2. The source IP address specified in system view.
3. The IP address of the outbound interface specified by the route.

Follow these steps to specify a source IP address for all HWTACACS schemes:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Specify a source IP address for outgoing HWTACACS packets | hwtacacs nas-ip <i>ip-address</i> | Required By default, the IP address of the outbound interface is used as the source IP address. |

Follow these steps to specify a source IP address for a specific HWTACACS scheme:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter HWTACACS scheme view | hwtacacs scheme <i>hwtacacs-scheme-name</i> | — |
| Specify a source IP address for outgoing HWTACACS packets | nas-ip <i>ip-address</i> | Required By default, the IP address of the outbound interface is used as the source IP address. |

Setting timers for controlling communication with HWTACACS servers

Follow these steps to set timers regarding HWTACACS servers:

| To do... | Use the command... | Remarks |
|--|--|-----------------------------------|
| Enter system view | system-view | — |
| Enter HWTACACS scheme view | hwtacacs scheme <i>hwtacacs-scheme-name</i> | — |
| Set the HWTACACS server response timeout timer | timer response-timeout <i>seconds</i> | Optional 5 seconds by default |
| Set the quiet timer for the primary server | timer quiet <i>minutes</i> | Optional 5 minutes by default |
| Set the real-time accounting interval | timer realtime-accounting <i>minutes</i> | Optional 12 minutes by default |

NOTE:

- For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. If the device does not receive any response to the information, it does not forcibly disconnect the online users.
- The real-time accounting interval must be a multiple of 3.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the HWTACACS server. A shorter interval requires higher performance.

Displaying and maintaining HWTACACS

| To do... | Use the command... | Remarks |
|---|---|------------------------|
| Display configuration information or statistics of HWTACACS schemes | display hwtacacs [<i>hwtacacs-server-name</i> [statistics]] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display information about buffered stop-accounting requests that get no responses | display stop-accounting-buffer hwtacacs-scheme <i>hwtacacs-scheme-name</i> [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Clear HWTACACS statistics | reset hwtacacs statistics { accounting all authentication authorization } [slot <i>slot-number</i>] | 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 device 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 access device.

To use remote authentication, authorization, and accounting, create the required RADIUS and HWTACACS schemes as described in “[Configuring RADIUS schemes](#)” and “[Configuring HWTACACS schemes](#).”

Creating an ISP domain

In a networking scenario with multiple ISPs, an access device may connect users of different ISPs. Because users of different ISPs may have different user attributes (for example, different username and password structure, service type, and rights), you must configure ISP domains to distinguish the users and configure different AAA methods for the ISP domains.

On a NAS, each user belongs to an ISP domain. A NAS can accommodate up to 16 ISP domains, including the factory default ISP domain, which is named **system**. If a user does not provide the ISP domain name at login, the system considers that the user belongs to the default ISP domain.

Follow these steps to create an ISP domain:

| To do... | Use the command... | Remarks |
|--|--|--|
| Enter system view | system-view | — |
| Create an ISP domain and enter ISP domain view | domain <i>isp-name</i> | Required |
| Return to system view | quit | — |
| Specify the default ISP domain | domain default enable <i>isp-name</i> | Optional By default, the default ISP domain is the factory default ISP domain system . |

NOTE:

To delete the default ISP domain, you must change it to a non-default ISP domain (with the **domain default disable** command) first.

Configuring ISP domain attributes

Follow these steps to configure ISP domain attributes:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter ISP domain view | domain <i>isp-name</i> | — |
| Place the ISP domain to the state of active or blocked | state { active block } | Optional By default, an ISP domain is in the active state, and users in the domain can request network services. |
| Specify the maximum number of active users in the ISP domain | access-limit enable <i>max-user-number</i> | Optional No limit by default |
| Configure the idle cut function | idle-cut enable <i>minute</i> [<i>flow</i>] | Optional Disabled by default This command is effective for only LAN users and portal users. |
| Configure the self-service server location function | self-service-url enable <i>url-string</i> | Optional Disabled by default |
| Specify the default authorization user profile | authorization-attribute user-profile <i>profile-name</i> | Optional By default, an ISP domain has no default authorization user profile. |

NOTE:

- If a user passes authentication but is authorized with no user profile, the device 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 the user profile, see the chapter "User profile configuration."
- A self-service RADIUS server, such as Intelligent Management Center (iMC), is required for the self-service server location function to work. With the self-service function, a user can manage and control his or her accounting information or card number. A server with self-service software is a self-service server.

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 features high speed and low cost, but the amount of information that can be stored is limited by the hardware.
- Remote authentication (**scheme**)—The access device cooperates with a RADIUS or HWTACACS server to authenticate users. The device can use the standard RADIUS protocol or extended RADIUS protocol in collaboration with systems like iMC to implement user authentication. Remote authentication features centralized information management, high capacity, high reliability, and support for centralized authentication service for multiple access devices. You can configure local or

no authentication as the backup method to be 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:

- For RADIUS or HWTACACS authentication, configure the RADIUS or HWTACACS scheme to be referenced first. The local and none authentication methods do not require any scheme.
- Determine the access mode or service type to be configured. With AAA, you can configure an authentication method for each access mode and service type, limiting the authentication protocols that can be used for access.
- Determine whether to configure an authentication method for all access modes or service types.

Follow these steps to configure AAA authentication methods for an ISP domain:

| To do... | Use the command... | Remarks |
|--|--|---|
| Enter system view | system-view | — |
| Enter ISP domain view | domain <i>isp-name</i> | — |
| Specify the default authentication method for all types of users | authentication default { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional local by default |
| Specify the authentication method for LAN users | authentication lan-access { local none radius-scheme <i>radius-scheme-name</i> [local none] } | Optional The default authentication method is used by default. |
| Specify the authentication method for login users | authentication login { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional The default authentication method is used by default. |
| Specify the authentication method for portal users | authentication portal { local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional The default authentication method is used by default. |
| Specify the authentication method for privilege level switching | authentication super { hwtacacs-scheme <i>hwtacacs-scheme-name</i> radius-scheme <i>radius-scheme-name</i> } | Optional The default authentication method is used by default. |

NOTE:

- 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 mode.
 - 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 does include the authorization information, but the authentication process ignores the information.
 - With the **radius-scheme** *radius-scheme-name* **local**, or **hwtacacs-scheme** *hwtacacs-scheme-name* **local** keyword and argument combination configured, 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 device 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 device 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 original username, the login username or the username entered by the user. 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.
-

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 access device performs no authorization exchange. After passing authentication, non-login users can access the network, FTP users can access the root directory of the device, and other login users have only the rights of Level 0 (visiting).
- Local authorization (**local**)—The access device performs authorization according to the user attributes configured for users.
- Remote authorization (**scheme**)—The access device cooperates with a RADIUS or an 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 to be 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 mode or service type to be configured. With AAA, you can configure an authorization scheme for each access mode and service type, limiting the authorization protocols that can be used for access.

- Determine whether to configure an authorization method for all access modes or service types.

Follow these steps to configure AAA authorization methods for an ISP domain:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Enter ISP domain view | domain <i>isp-name</i> | — |
| Specify the default authorization method for all types of users | authorization default { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional local by default |
| Specify the command authorization method | authorization command { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local none] local none } | Optional The default authorization method is used by default. |
| Specify the authorization method for LAN users | authorization lan-access { local none radius-scheme <i>radius-scheme-name</i> [local none] } | Optional The default authorization method is used by default. |
| Specify the authorization method for login users | authorization login { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional The default authorization method is used by default. |
| Specify the authorization method for portal users | authorization portal { local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional The default authorization method is used by default. |

NOTE:

- 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 mode.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. In addition, if a RADIUS authorization fails, the error message returned to the NAS says that the server is not responding.
- With the **radius-scheme** *radius-scheme-name* **local**, or **hwtacacs-scheme** *hwtacacs-scheme-name* [**local** | **none**] keyword and argument combination configured, 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 device has no backup authorization method and performs only local authorization or does not perform any authorization.
- The authorization information from the RADIUS server is sent to the RADIUS client along with the authentication response message. You cannot specify a separate RADIUS authorization server. If you use RADIUS for authorization and authentication, you must use the same scheme setting for authorization and authentication; otherwise, the system will display an error message.

Configuring AAA accounting methods for an ISP domain

In AAA, accounting is a separate process at the same level as authentication and authorization. Its responsibility is to send accounting start/update/end requests to the specified accounting server. Accounting is not required, and accounting method configuration 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 access device. It is for counting and controlling 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 access device cooperates with a RADIUS server or HWTACACS server for accounting of users. You can configure local or no accounting as the backup method to be 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 authentication methods do not require any scheme.
2. Determine the access mode or service type to be configured. With AAA, you can configure an accounting method for each access mode and service type, limiting the accounting protocols that can be used for access.
3. Determine whether to configure an accounting method for all access modes or service types.

Follow these steps to configure AAA accounting methods for an ISP domain:

| To do... | Use the command... | Remarks |
|--|--|---|
| Enter system view | system-view | — |
| Enter ISP domain view | domain <i>isp-name</i> | — |
| Enable the accounting optional feature | accounting optional | Optional Disabled by default |
| Specify the default accounting method for all types of users | accounting default { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional local by default |
| Specify the command accounting method | accounting command hwtacacs-scheme <i>hwtacacs-scheme-name</i> | Optional The default accounting method is used by default. |
| Specify the accounting method for LAN users | accounting lan-access { local none radius-scheme <i>radius-scheme-name</i> [local none] } | Optional The default accounting method is used by default. |
| Specify the accounting method for login users | accounting login { hwtacacs-scheme <i>hwtacacs-scheme-name</i> [local] local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional The default accounting method is used by default. |
| Specify the accounting method for portal users | accounting portal { local none radius-scheme <i>radius-scheme-name</i> [local] } | Optional The default accounting method is used by default. |

NOTE:

- With the **accounting optional** command configured, a user that would be otherwise disconnected can still use the network resources even when no accounting server is available or communication with the current accounting server fails.
 - The local accounting method is not used to implement accounting, but to work together with the **access-limit** command, which is configured in local user view, to limit the number of local user connections. However, with the **accounting optional** command configured, 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 mode.
 - With the **radius-scheme** *radius-scheme-name* **local** or **hwtacacs-scheme** *hwtacacs-scheme-name* **local** keyword and argument combination configured, 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 device has no backup accounting method and performs only local accounting or does not perform any accounting.
 - Accounting is not supported for FTP services.
-

Tearing down user connections forcibly

Follow these steps to tear down user connections forcibly:

| To do... | Use the command... | Remarks |
|---|--|---|
| Enter system view | system-view | — |
| Tear down AAA user connections forcibly | cut connection { access-type { dot1x mac-authentication portal } all domain <i>isp-name</i> interface <i>interface-type interface-number</i> ip ip-address mac <i>mac-address</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i> vlan <i>vlan-id</i> } [slot <i>slot-number</i>] | Required Applicable to only LAN access, and portal user connections. |

Configuring a network device 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 network device 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 device.

Follow these steps to configure a RADIUS user:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Create a RADIUS user and enter RADIUS server user view | radius-server user <i>user-name</i> | Required No RADIUS user exists by default. |
| Configure a password for the RADIUS user | password [cipher simple] <i>password</i> | Optional By default, no password is specified. |
| Configure the authorization attribute for the RADIUS user | authorization-attribute { acl <i>acl-number</i> vlan <i>vlan-id</i> } * | Optional Not configured by default. |
| Configure the expiration time for the RADIUS user | expiration-date <i>time</i> | Optional By default, no expiration time is configured, and the system does not check users' expiration time. |
| Configure a description for the RADIUS user | description <i>text</i> | Optional Not configured by default. |

NOTE:

You can use the **authorization-attribute** command to specify an authorization ACL and authorized VLAN, which will be 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 will fail and the NAS will log the RADIUS user out forcibly. If the assigned VLAN does not exist on the NAS, the NAS will create the VLAN and add the RADIUS user or the access port to the VLAN.

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.

Follow these steps to specify a RADIUS client

| To do... | Use the command... | Remarks |
|-------------------------|---|---|
| Enter system view | system-view | — |
| Specify a RADIUS client | radius-server client-ip <i>ip-address</i> [key <i>string</i>] | Required 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 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

| To do... | Use the command... | Remarks |
|--|---|-----------------------|
| Display the configuration information of ISP domains | display domain [<i>isp-name</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display information about user connections | display connection [access-type { dot1x mac-authentication portal } domain <i>isp-name</i> interface <i>interface-type interface-number</i> ip <i>ip-address</i> mac <i>mac-address</i> ucibindex <i>ucib-index</i> user-name <i>user-name</i> vlan <i>vlan-id</i>] [slot <i>slot-number</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

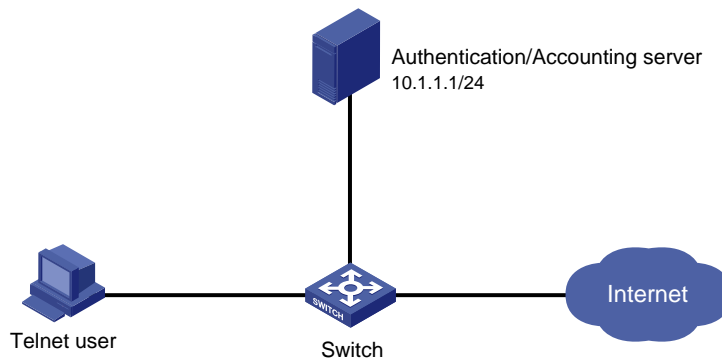
AAA configuration examples

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 authentication, authorization, and accounting packets exchanged with the HWTACACS server to **expert**. Specify that the switch remove the domain names in usernames before sending usernames to the HWTACACS server.

Figure 10 Configure AAA for Telnet users by an HWTACACS server



Configuration procedure

Configure the IP addresses of the interfaces (omitted).

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 key for authentication, authorization, and accounting packets to expert.
[Switch-hwtacacs-hwtac] key authentication expert
[Switch-hwtacacs-hwtac] key authorization expert
[Switch-hwtacacs-hwtac] key accounting expert

# Configure the scheme to remove the domain names in usernames before sending usernames to the
HWTACACS server.
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit

# Configure the AAA methods for the domain, or set default AAA methods for all types of users in 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

Or
[Switch] domain bbb
[Switch-isp-bbb] authentication default hwtacacs-scheme hwtac
[Switch-isp-bbb] authorization default hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting default hwtacacs-scheme hwtac

When telnetting to the switch, a user enters username userid@bbb for authentication using domain bbb.

```

AAA for Telnet users by separate servers

Network requirements

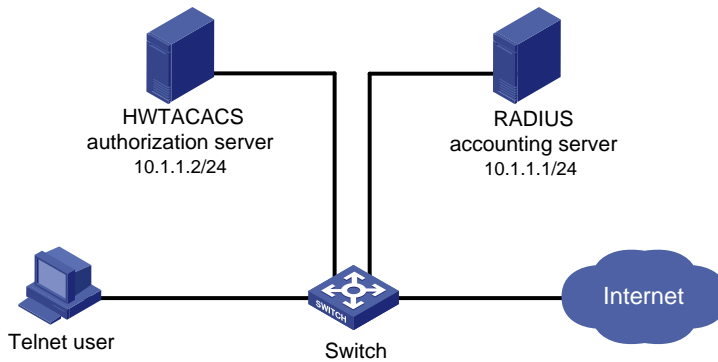
As shown in [Figure 11](#), configure the switch to provide local authentication, HWTACACS authorization, and RADIUS accounting services for Telnet users. The username and the password for Telnet users are both **hello**.

Set the shared keys for packets exchanged with the HWTACACS server and the RADIUS server to **expert**. Configure the switch to remove the domain names in usernames before sending usernames to the servers.

NOTE:

Configuration of separate AAA for other types of users is similar to that given in this example. The only difference is in the access type.

Figure 11 Configure AAA by separate servers for Telnet users



Configuration procedure

Configure the IP addresses of various interfaces (omitted).

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, or set default AAA methods for all types of users in the 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
```


Or

```
[Switch] domain bbb
[Switch-isp-bbb] authentication default local
[Switch-isp-bbb] authorization default hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting default radius-scheme rd
```

When telnetting to the switch, a user enters username **telnet@bbb** for authentication using domain **bbb**.

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

NOTE:

The configuration of authentication and authorization for SSH users is similar to that for Telnet users. The following takes SSH users as an example.

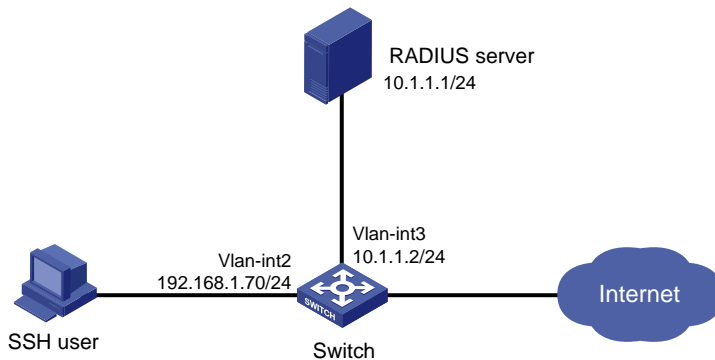
Network requirements

As shown in [Figure 12](#), configure an iMC server to act as the RADIUS server to provide authentication and authorization services for SSH users.

Set both the shared keys for packets exchanged with the RADIUS server to **expert**, and configure the switch to include the domain names in usernames to be sent to the RADIUS server.

Add an account on the RADIUS server, with the username **hello@bbb**. The SSH user uses the username and the configured password to log in to the switch and is authorized with the privilege level of 3 after login.

Figure 12 Configure authentication/authorization for SSH users by a RADIUS server



Configuration procedure

1. Configure the RADIUS server (iMC PLAT 5.0)

NOTE:

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

Add an access device.

Log in to the iMC management platform, select the **Service** tab, and select **User Access Manager > Access Device** from the navigation tree to enter the **Access Device** page. Then, click **Add** to enter the **Add Access Device** window and perform the following configurations as shown in [Figure 13](#).

- Set the shared key for authentication and accounting to **expert**

- Specify the ports for authentication and accounting as 1812 and 1813 respectively
- Select **Device Management Service** as the service type
- Select **HP(A-Series)** as the access device type
- Select the access device from the device list or manually add the device with the IP address of 10.1.1.2
- Click **OK** to finish the operation

NOTE:

The IP address of the access device specified above must be the same as the source IP address of the RADIUS packets sent from the device, 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 device.

Figure 13 Add 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 Service |
| Access Device Type | HP(A-Series) | 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 | | X |

OK Cancel

Add a user for device management

Log in to the iMC management platform, select the **User** tab, and select **Device Management User** from the navigation tree to enter the **Device Management User** page. Then, click **Add** to enter the **Add Device Management User** window and perform the following configurations as shown in [Figure 14](#).

- Add a user named **hello@bbb** and specify 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 to 10.1.1.255
- Click **OK** to finish the operation

Figure 14 Add 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: ?

* User Password:

* Confirm Password:

Service Type: ▼

EXEC Priority: ?

Bound User IP List

No match found.

| <input type="checkbox"/> | Start IP | End IP | Delete |
|--------------------------|----------|--------|--------|
|--------------------------|----------|--------|--------|

IP Address List of Managed Devices

Total Items: 1.

| <input type="checkbox"/> | Start IP | End IP | Delete |
|--------------------------|----------|------------|--------|
| <input type="checkbox"/> | 10.1.1.0 | 10.1.1.255 | ✖ |

2. Configure the switch

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

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

Configure the IP address of VLAN-interface 3, through which the switch 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 authentication packets 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 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

```

3. Verify 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.

```

AAA for 802.1X users by a RADIUS server

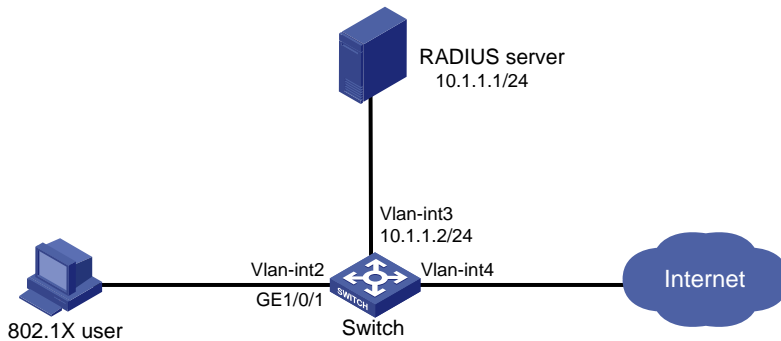
Network requirements

As shown in [Figure 15](#), configure the switch to use the RADIUS server to perform authentication, authorization, and accounting for 802.1X users. Set the shared keys for authentication and authorization packets exchanged between the switch and the RADIUS server to **expert** and set the ports for authentication/authorization and accounting to 1812 and 1813 respectively. Configure the switch to include the domain names in usernames to be sent to the RADIUS server.

Configure MAC-based access control on GigabitEthernet 1/0/1 to authenticate all 802.1X users on the port separately.

Configure an account for the user, with the username dot1x@bbb. Configure the authentication server to assign the host to VLAN 4 after the host passes authentication. Register a monthly service that charges 120 dollars for up to 120 hours per month for the user.

Figure 15 Configure AAA for 802.1X users by a RADIUS server



Configuration procedure

NOTE:

- Configure the interfaces and VLANs as shown in Figure 15. Make sure that the host can get a new IP address manually or automatically and can access resources in the authorized VLAN after passing authentication.

1. Configure the RADIUS server (iMC PLAT 5.0)

NOTE:

This example assumes that the RADIUS server runs iMC PLAT 5.0 (E0101), iMC UAM 5.0 (E0101), and iMC CAMS 5.0 (E0101).

Add an access device.

Log in to the iMC management platform, select the **Service** tab, and select **User Access Manager > Access Device** from the navigation tree to enter the **Access Device List** page. Then, click **Add** to enter the **Add Access Device** page and perform the following configurations:

- Set the shared key for authentication and accounting to **expert**
- Specify the ports for authentication and accounting as 1812 and 1813 respectively
- Select **LAN Access Service** as the service type
- Select **HP(A-Series)** as the access device type
- Select the access device from the device list or manually add the device whose IP address is 10.1.1.2
- Adopt the default settings for other parameters and click **OK** to finish the operation.

NOTE:

The IP address of the access device specified above must be the same as the source IP address of the RADIUS packets sent from the device, 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 access device.

Figure 16 Add an access device

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

Access Configuration

| | | | |
|--------------------|-------------------------------------|-----------------------|-----------------------------------|
| * Shared Key | <input type="text" value="expert"/> | * Authentication Port | <input type="text" value="1812"/> |
| * Accounting Port | <input type="text" value="1813"/> | Service Type | LAN Access Service |
| Access Device Type | HP(A-Series) | 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 | | ✘ |

OK Cancel

Add a charging policy.

Select the **Service** tab, and select **Accounting Manager > Charging Plans** from the navigation tree to enter the charging policy configuration page. Then, click **Add** to enter the **Add Charging Plan** page and perform the following configurations:

- Add a plan named **UserAcct**
- Select **Flat rate** as the charging template
- In the **Basic Plan Settings** field, configure to charge the fixed fee of 120 dollars per month
- In the **Service Usage Limit** field, set the **Usage Threshold** to 120 hours, allowing the user to access the Internet for up to 120 hours per month
- Adopt the default settings for other parameters and click **OK** to finish the operation.

Figure 17 Add a charging policy

Service >> Accounting Manager >> Charging Plans >> Add Charging Plan

Charging Plan Setup

Basic Information

| | |
|-------------------|---------------------------------------|
| * Plan Name | <input type="text" value="UserAcct"/> |
| Charging Template | Flat rate |
| Service Group | Ungrouped |
| Description | <input type="text"/> |

Basic Plan Settings

| | |
|-----------------|---|
| Charge Based on | time |
| Billing Term | Monthly |
| * Fixed Fee | <input type="text" value="120"/> dollar |

Service Usage Limit

| | | | |
|-----------------|----------------------------------|----|---------------------------------|
| Usage Threshold | <input type="text" value="120"/> | in | <input type="text" value="hr"/> |
|-----------------|----------------------------------|----|---------------------------------|


OK Cancel

Add a service.

Select the **Service** tab, and select **User Access Manager > Service Configuration** from the navigation tree to enter the **Service Configuration** page. Then, click **Add** to enter the **Add Service Configuration** page and perform the following configurations:

- Add a service named **Dot1x auth** and set the **Service Suffix** to **bbb**, which indicates the authentication domain for the 802.1X user. With the service suffix configured, you must configure usernames to be sent to the RADIUS service to carry the domain name.
- Specify **UserAcct** as the **Charging Plan**.
- Select **Deploy VLAN** and set the ID of the VLAN to be assigned to 4.
- Configure other parameters according to the actual situation.
- Click **OK** to finish the operation.

Figure 18 Add a service

 [Service](#) >> [User Access Manager](#) >> [Service Configuration](#) >> [Add Service Configuration](#)

Add Service Configuration

Basic Information

| | | | |
|---|---|---|--|
| * Service Name | <input type="text" value="Dot1x auth"/> | Service Suffix | <input type="text" value="bbb"/> |
| * Service Group | <input type="text" value="Ungrouped"/> | | |
| Charging Plan | <input type="text" value="UserAcct"/> | | |
| Billing Term Start Type | <input type="text" value="Auto"/> | Start Date | <input type="text" value="Unlimited"/> |
| <input type="checkbox"/> Adaptive consecutive deduction | <input checked="" type="radio"/> Charge Whole Term in Initial Term <input type="radio"/> Charge by Day in Initial Term <input type="radio"/> No Charge for Initial Term | | |
| Description | <input type="text"/> | | |
| LDAP Priority | <input type="text"/> | <input checked="" type="checkbox"/> Available ? | |

Authorization Information

| | | | |
|---|---|--|---------------------------------|
| * Access Period | <input type="text" value="None"/> | Allocate IP | <input type="text" value="No"/> |
| Downstream Rate | <input type="text"/> Kbps | Upstream Rate | <input type="text"/> Kbps |
| Priority | <input type="text"/> | <input type="checkbox"/> RSA Authentication | |
| Certificate Authentication | <input checked="" type="radio"/> None <input type="radio"/> EAP | | |
| Certificate Type | <input type="text" value="EAP-TLS AuthN"/> | | |
| <input checked="" type="checkbox"/> Deploy VLAN | <input type="text" value="4"/> | <input type="checkbox"/> Deploy User Profile | <input type="text"/> |
| <input type="checkbox"/> Deploy User Group | <input type="text"/> ? | | |
| <input type="checkbox"/> Deploy ACL | | | |

Add a user.

Select the **User** tab, and select **All Access Users** from the navigation tree to enter the **All Access Users** page. Then, click **Add** to enter the **Add Access User** page and perform the following configurations:

- Select the user or add a user named **test**
- Specify the account name as **dot1x** and configure the password
- Select the access service **Dot1x auth**
- Configure other parameters accordingly and click **OK** to finish the operation

Figure 19 Add an access user account

User >> All Access Users >> Add Access User Help

Access account

Access Information

* User Name:

* Account Name: Fast Access User Computer User

* Password: * Confirm Password:

Allow User to Change Password Enable Password Strategy Modify Password at Next Login

Expiration Date:

Max. Idle Time: Minutes Max. Concurrent Logins:

Account Type: * Prepaid Money: dollar

Self-Service Recharge:

Login Message:

Access Service

| | Service Name | Service Suffix | Status | Charging Plan | Allocate IP |
|-------------------------------------|--------------|----------------|-----------|---------------|-------------|
| <input checked="" type="checkbox"/> | Dot1x auth | bbb | Available | UserAcct | |

2. Configure the switch

- Configure a RADIUS scheme

Create a RADIUS scheme named **rad** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rad
```

Set the server type for the RADIUS scheme. When using the iMC server, set the server type to **extended**.

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

Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rad] primary authentication 10.1.1.1
[Switch-radius-rad] primary accounting 10.1.1.1
[Switch-radius-rad] key authentication expert
[Switch-radius-rad] key accounting 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
[Switch-radius-rad] quit
```

- Configure an authentication domain

Create an ISP domain named **bbb** and enter its view.

```
[Switch] domain bbb
```

Configure the ISP domain to use RADIUS scheme **rad**.

```
[Switch-isp-bbb] authentication lan-access radius-scheme rad
[Switch-isp-bbb] authorization lan-access radius-scheme rad
[Switch-isp-bbb] accounting lan-access radius-scheme rad
[Switch-isp-bbb] quit
```


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

```
[Switch] domain default enable bbb
```

- Configure 802.1X authentication

Enable 802.1X globally.

```
[Switch] dot1x
```

Enable 802.1X for port GigabitEthernet 1/0/1.

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] dot1x
```

```
[Switch-GigabitEthernet1/0/1] quit
```

Configure the access control method. (Optional. The default setting meets the requirement.)

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

3. Verification

NOTE:

- If the 802.1X client of Windows XP is used, the properties of the 802.1X connection should be specifically configured in the **Authentication** tab on the **Properties** page, where you must select the **Enable IEEE 802.1X authentication for this network** option and specify the **EAP type** as **MD5-Challenge**.
 - If the iNode client is used, no advanced authentication options need to be enabled.
-

When using the iNode client, the user can pass authentication after entering username **dot1x@bbb** and the correct password in the client property page. When using the Windows XP 802.1X client, the user can pass authentication after entering the correct username and password in the pop-up authentication page. After the user passes authentication, the server assigns the port connecting the client to VLAN 4.

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

```
[Switch] display connection
```

```
Slot: 1
```

```
Index=22 , Username=dot1x@bbb
```

```
IP=192.168.1.58
```

```
IPv6=N/A
```

```
MAC=0015-e9a6-7cfe
```

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

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

View the information of the specified connection on the switch.

```
[Switch] display connection ucibindex 22
```

```
Slot: 1
```

```
Index=22 , Username=dot1x@bbb
```

```
MAC=0015-e9a6-7cfe
```

```
IP=192.168.1.58
```

```
IPv6=N/A
```

```
Access=8021X , AuthMethod=CHAP
```

```
Port Type=Ethernet, Port Name=GigabitEthernet1/0/1
```

```
Initial VLAN=2, Authorized VLAN=4
```

```
ACL Group=Disable
```

```
User Profile=N/A
```

```
CAR=Disable
```

```
Priority=Disable
Start=2011-04-26 19:41:12 ,Current=2011-04-26 19:41:25 ,Online=00h00m14s
Total 1 connection matched.
```

As the **Authorized VLAN** field in the output shows, VLAN 4 has been assigned to the user.

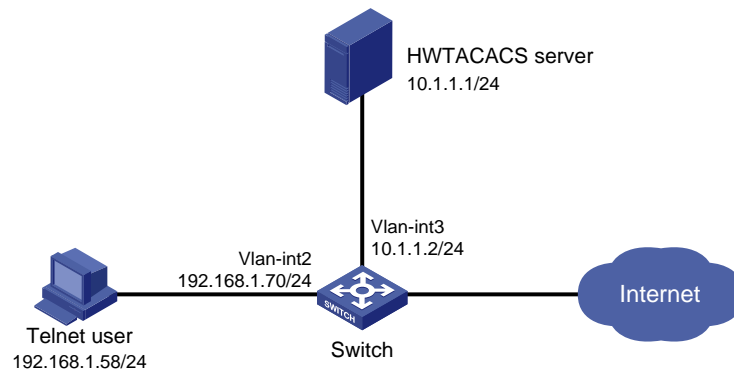
Level switching authentication for Telnet users by an HWTACACS server

Network requirements

As shown in Figure 20, 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.

Configure the switch to use the HWTACACS server for level switching authentication of the Telnet user, and to use local authentication as the backup method.

Figure 20 Configure level switching authentication for Telnet users by an HWTACACS server



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 privilege level for the user to enjoy after login.
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 authentication packets to expert.
[Switch-hwtacacs-hwtac] key authentication expert

# Configure the scheme to remove the domain names in usernames before sending usernames 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 **tester** on the HWTACACS server and configure advanced attributes for the user as follows and as shown in [Figure 21](#):

- Select **Max Privilege for any AAA Client** and set the privilege level to level 3. After these configurations, the user needs to use the password **enabpass** when switching to level 1, level 2, or level 3.
- Select **Use separate password** and specify the password as **enabpass**.

Figure 21 Configure 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: [masked]
Confirm Password: [masked]

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

Password: [masked]
Confirm Password: [masked]

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 **aabbbc** 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) 2010-2011 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:

```
cluster Run cluster command
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

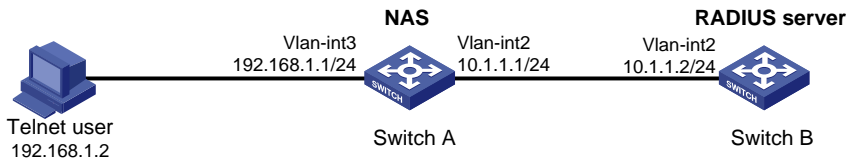
RADIUS authentication and authorization for Telnet users by a network device

Network requirements

As shown in [Figure 22](#), configure Switch B to act as a RADIUS server to provide authentication and authorization for the Telnet user on port 1645.

Set the shared keys for authentication and authorization packets exchanged between the NAS and the RADIUS server to **abc**. Configure the switch to remove the domain names in usernames before sending usernames to the RADIUS server.

Figure 22 RADIUS authentication and authorization for Telnet users by a network device



Configuration procedure

Configure an IP address for each interface as shown in [Figure 22](#). The detailed configuration is omitted here.

1. 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 authentication packets as **abc**.

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

Configure the scheme to remove the domain names in usernames before sending usernames to the RADIUS server.

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

Specify 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 network device 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 will be used for the user.

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

2. Configure the RADIUS server

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

```
<SwitchB> system-view
```

```
[SwitchB] radius-server user aaa
```

Configure simple-text 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 shared key as **abc**.

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

Verification

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 no default ISP domain is specified for 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 a default ISP domain is specified 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 communication link between the NAS and the RADIUS server is down (at the physical layer and data link layer).
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 fundamentals

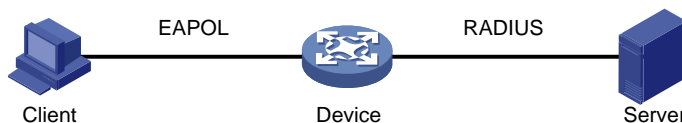
802.1X is a port-based network access control protocol initially proposed by the IEEE 802 LAN/WAN committee for securing wireless LANs (WLANs), and it has also been widely used on Ethernet networks for access control.

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: client (the supplicant), network access device (the authenticator), and the authentication server.

Figure 23 802.1X architecture



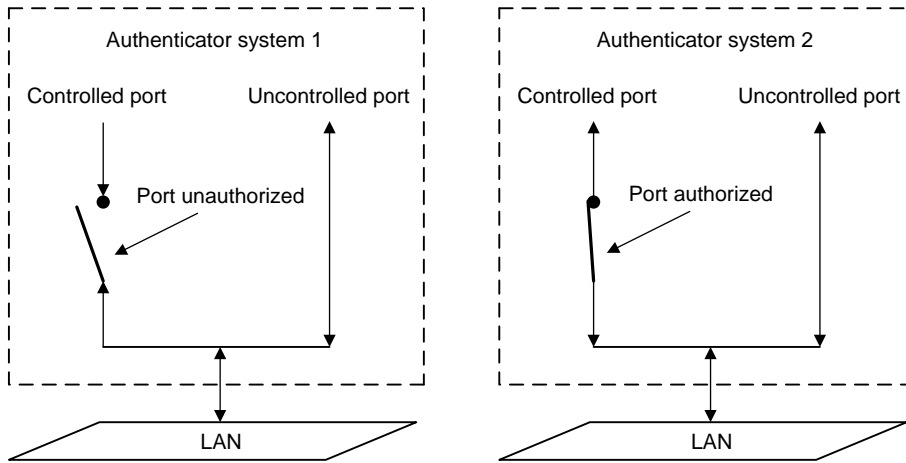
- The client is a user terminal seeking access to the LAN. It must have 802.1X software to authenticate to the network access device.
- The network access device authenticates the client to control access to the LAN. In a typical 802.1X environment, the network access device uses an authentication server to perform authentication.
- The authentication server is the entity that 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.

- The 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 24](#). 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.
- The uncontrolled port is always open to receive and transmit EAPOL frames.

Figure 24 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.

NOTE:

The HP switches 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:

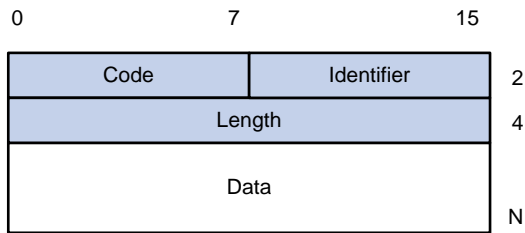
- Encapsulates EAP packets in RADIUS by using EAP over RADIUS (EAPOR), as described in “[EAP relay](#).”
- Extracts authentication information from the EAP packets and encapsulates the information in standard RADIUS packets, as described in “[EAP termination](#).”

Packet format

EAP packet format

Figure 25 shows the EAP packet format.

Figure 25 EAP packet format

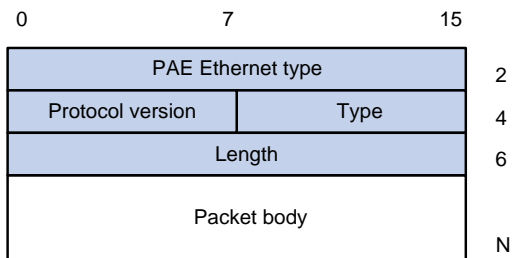


- Code: Type of the EAP packet. Options include Request (1), Response (2), Success (3), or Failure (4).
- Identifier: Used for matching Responses with Requests.
- Length: Length (in bytes) of the EAP packet, which is the sum of the Code, Identifier, Length, and Data fields.
- Data: Content of the EAP 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 26 shows the EAPOL packet format.

Figure 26 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 that the HP implementation of 802.1X supports.

Table 5 Types of EAPOL packets

| 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. |
| 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.

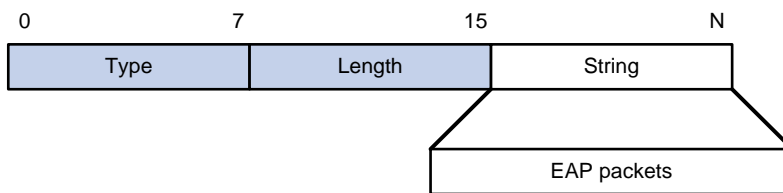
EAP over RADIUS

RADIUS adds two attributes, EAP-Message and Message-Authenticator, for supporting EAP authentication. For the RADIUS packet format, see the chapter “AAA configuration.”

EAP-Message

RADIUS encapsulates EAP packets in the EAP-Message attribute, as shown in Figure 27. 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.

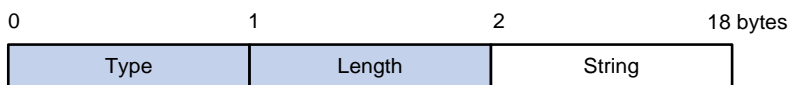
Figure 27 EAP-Message attribute format



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 28 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 can be 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 this multicast address, you must use an 802.1X client, the 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:

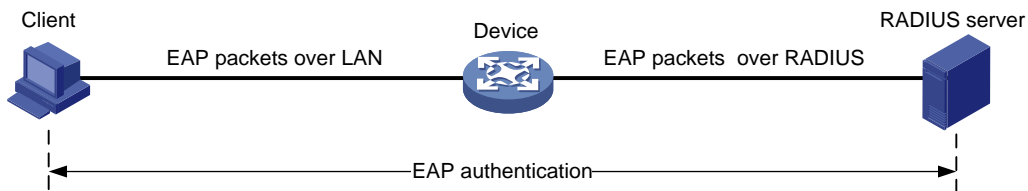
- Multicast trigger mode—The access device multicasts EAP-Request/Identify packets periodically (every 30 seconds by default) to initiate 802.1X authentication.
- Unicast trigger mode—Upon receiving a frame with the source MAC address not in the MAC address table, the access device sends an EAP-Request/Identify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

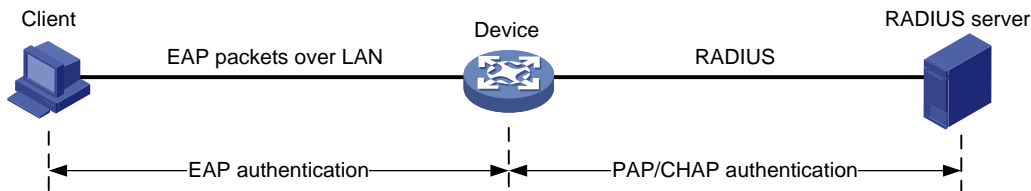
EAP relay is defined in IEEE 802.1X. In this mode, the network device uses EAPoR packets to send authentication information to the RADIUS server, as shown in [Figure 29](#).

Figure 29 EAP relay



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 30](#).

Figure 30 EAP termination



A comparison of EAP relay and EAP termination

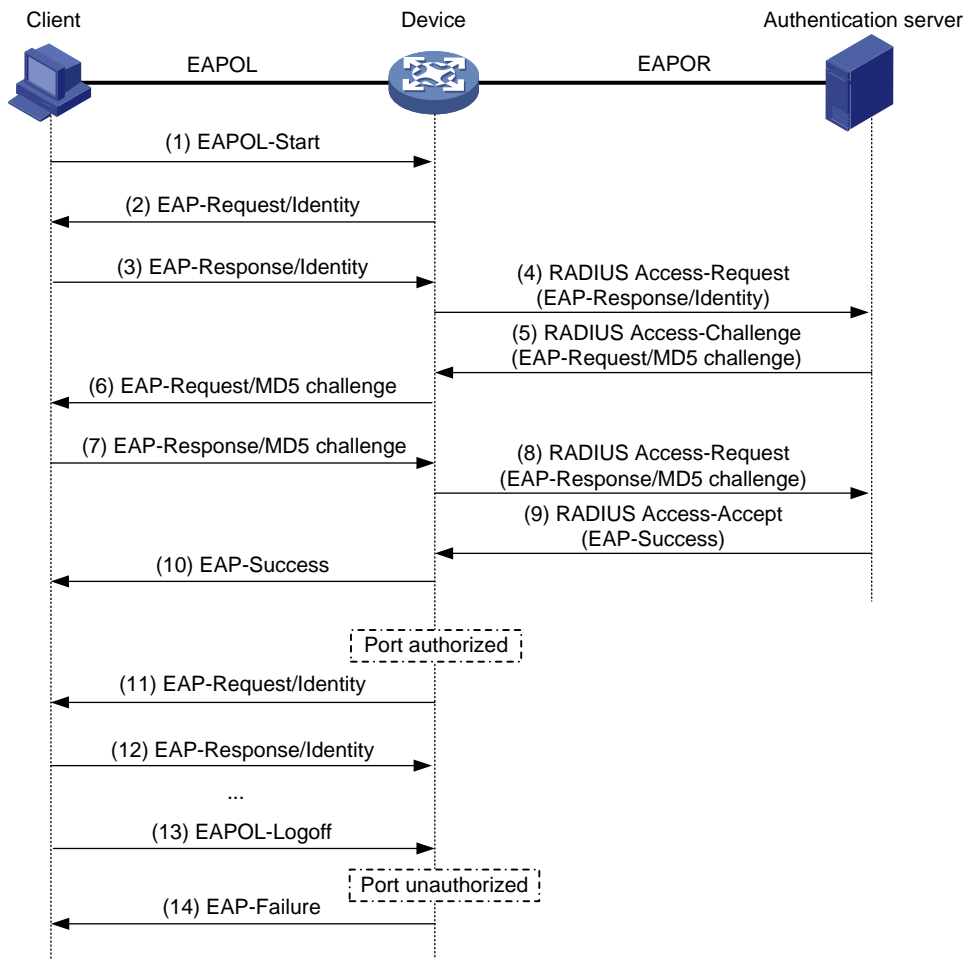
| Packet exchange method | Benefits | Limitations |
|------------------------|---|--|
| EAP relay | <ul style="list-style-type: none"> • Supports various EAP authentication methods. • The configuration and processing is simple on the network access device | The RADIUS server must support the EAP-Message and Message-Authenticator attributes, and the EAP authentication method used by the client. |

| Packet exchange method | Benefits | Limitations |
|------------------------|--|---|
| EAP termination | Works with any RADIUS server that supports PAP or CHAP authentication. | <ul style="list-style-type: none"> Supports only MD5-Challenge EAP authentication and the "username + password" EAP authentication initiated by an iNode 802.1X client. The processing is complex on the network access device. |

EAP relay

Figure 31 shows the basic 802.1X authentication procedure in EAP relay mode, assuming that EAP-MD5 is used.

Figure 31 802.1X authentication procedure in EAP relay mode



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.
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.

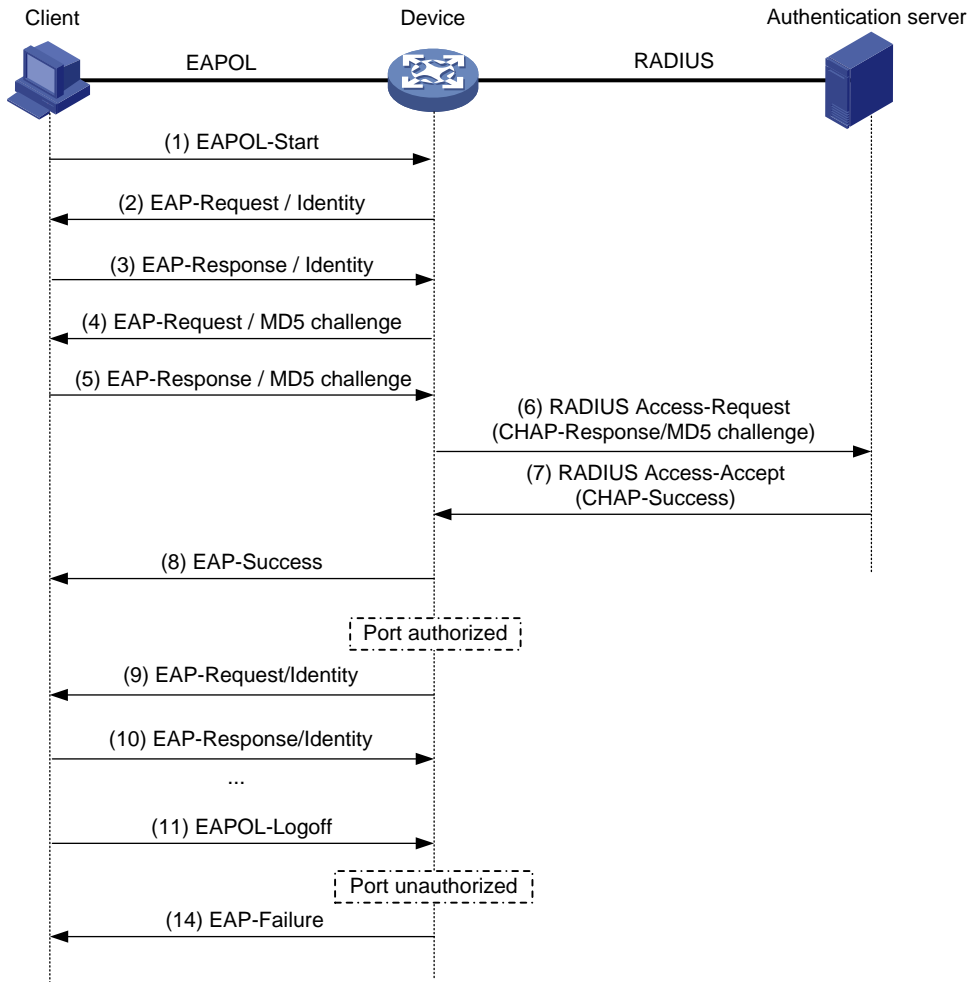
NOTE:

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.

EAP termination

Figure 32 shows the basic 802.1X authentication procedure in EAP termination mode, assuming that CHAP authentication is used.

Figure 32 802.1X 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.

802.1X configuration

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, for example, that requires different authentication methods for different users on a port. Port security is beyond the scope of this chapter. It is described in the chapter “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.

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

For more information about the fundamentals of 802.1X, see the chapter “802.1X fundamentals.”

Using 802.1X authentication with other features

VLAN assignment

You can configure the authentication server to assign a VLAN for an 802.1X user that has passed authentication. The way that the network access device handles VLANs on an 802.1X-enabled port differs by 802.1X access control mode.

| Access control | VLAN manipulation |
|----------------|---|
| Port-based | Assigns the VLAN to the port as the default VLAN. All subsequent 802.1X users can access the default VLAN without authentication. When the user logs off, the previous default VLAN restores, and all other online users are logged off. |

| Access control | VLAN manipulation |
|----------------|--|
| MAC-based | <ul style="list-style-type: none"> If the port is a hybrid port with MAC-based VLAN enabled, maps the MAC address of each user to the VLAN assigned by the authentication server. The default VLAN of the port does not change. When a user logs off, the MAC-to-VLAN mapping for the user is removed. Assigns the VLAN of the first authenticated user to the port as the default VLAN. If a different VLAN is assigned for a subsequent user, the user cannot pass the authentication. |

! **IMPORTANT:**

- With 802.1X authentication, a hybrid port is always assigned to a VLAN as an untagged member. After the assignment, do not re-configure the port as a tagged member in the VLAN.
- On a periodic online user re-authentication enabled port, if a user has been online before you enable the MAC-based VLAN function, the access 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 the *Layer 2—LAN Switching Configuration Guide*.

Guest VLAN

You can configure a guest VLAN to accommodate users that have not performed 802.1X authentication on a port, 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.

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

| Authentication status | VLAN manipulation |
|--|--|
| No 802.1X user has performed authentication or passed authentication within 90 seconds after 802.1X is enabled | <p>Assigns the 802.1X guest VLAN to the port as the default VLAN. All 802.1X users on this port can access only resources in the guest VLAN.</p> <p>If no 802.1X guest VLAN is configured, the access device does not perform any VLAN operation.</p> |
| A user in the 802.1X guest VLAN fails 802.1X authentication | <p>If an 802.1X Auth-Fail VLAN (see “Auth-Fail VLAN”) is available, assigns the Auth-Fail VLAN to the port as the default VLAN. All users on this port can access only resources in the Auth-Fail VLAN.</p> <p>If no Auth-Fail VLAN is configured, the default VLAN on the port is still the 802.1X guest VLAN. All users on the port are in the guest VLAN.</p> |
| A user in the 802.1X guest VLAN passes 802.1X authentication | <ul style="list-style-type: none"> Assigns the VLAN specified for the user to the port as the default VLAN, and removes the port from the 802.1X guest VLAN. After the user logs off, the user configured default VLAN restores. If the authentication server assigns no VLAN, the user configured default VLAN applies. The user and all subsequent 802.1X users are assigned to the user-configured default VLAN. After the user logs off, the default VLAN remains unchanged. |

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

| 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 default VLAN on the port. |

NOTE:

- To use the 802.1X guest VLAN function on a port that performs MAC-based access control, ensure that the port is a hybrid port, and enable MAC-based VLAN on the port.
- The network device assigns a hybrid port to an 802.1X guest VLAN as an untagged member.
- For more information about VLAN configuration and MAC-based VLAN, see the *Layer 2—LAN Switching Configuration Guide*.

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.

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 default VLAN. 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 default VLAN on the port, and all 802.1X users on this port are in this VLAN. |
| A user passes 802.1X authentication | <ul style="list-style-type: none"> • Assigns the VLAN specified for the user to the port as the default VLAN, and removes the port from the Auth-Fail VLAN. After the user logs off, the user-configured default VLAN restores. • If the authentication server assigns no VLAN, the initial default VLAN applies. The user and all subsequent 802.1X users are assigned to the user-configured default VLAN. After the user logs off, the default VLAN remains unchanged. |

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

| 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 default VLAN on the port. |

NOTE:

- To perform the 802.1X Auth-Fail VLAN function on a port that performs MAC-based access control, you must ensure that the port is a hybrid port, and enable MAC-based VLAN on the port.
- The network device assigns a hybrid port to an 802.1X Auth-Fail VLAN as an untagged member.
- For more information about VLAN configuration and MAC-based VLAN, see the *Layer 2—LAN Switching Configuration Guide*.

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.

Configuring 802.1X

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**.

For more information about RADIUS client configuration, see the chapter “AAA configuration.”

802.1X configuration task list

Complete the following tasks to configure 802.1X:

| Task | Remarks |
|---|----------|
| Enabling 802.1X | Required |
| Specifying EAP relay or EAP termination | Optional |

| Task | Remarks |
|---|----------|
| 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 |
| Enabling the quiet timer | Optional |
| Enabling the periodic online user re-authentication function | Optional |
| Configuring an 802.1X guest VLAN | Optional |
| Configuring an Auth-Fail VLAN | Optional |

Enabling 802.1X

NOTE:

- If the default VLAN of a port is a voice VLAN, the 802.1X function cannot take effect on the port. For more information about voice VLANs, see the *Layer 2—LAN Switching Configuration Guide*.
- 802.1X is mutually exclusive with link aggregation group configuration on a port.

Follow these steps to enable 802.1X on a port:

| To do... | Use the command... | Remarks |
|-------------------------|---|--|
| Enter system view | system-view | — |
| Enable 802.1X globally | dot1x | Required Disabled by default. |
| Enable 802.1X on a port | In system view dot1x interface interface-list | Required |
| | In Layer 2 Ethernet interface view interface interface-type interface-number dot1x | Use either approach. Disabled by default. |

Specifying EAP relay or EAP termination

When configuring 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 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."

Follow these steps to configure EAP relay or EAP termination:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Configure EAP relay or EAP termination | dot1x authentication-method { chap eap pap } | <p>Optional</p> <p>By default, the network access device performs EAP termination and uses CHAP to communicate with the RADIUS server.</p> <p>Specify the eap keyword to enable EAP termination.</p> <p>Specify the chap or pap keyword to enable CHAP-enabled or PAP-enabled EAP relay.</p> |

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. For more information about the **user-name-format** command, see the *Security Command Reference*.

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

Follow these steps to set the authorization state of a port:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | | Use the command... | Remarks |
|----------------------------------|------------------------------------|---|--|
| Set the port authorization state | In system view | dot1x port-control { authorized-force auto unauthorized-force } [interface interface-list] | Optional |
| | In Layer 2 Ethernet interface view | interface interface-type interface-number dot1x port-control { authorized-force auto unauthorized-force } | Use either approach. By default, auto applies. |

Specifying an access control method

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

Follow these steps to specify the access control method:

| To do... | | Use the command... | Remarks |
|----------------------------------|------------------------------------|---|---|
| Enter system view | | system-view | — |
| Specify an access control method | In system view | dot1x port-method { macbased portbased } [interface interface-list] | Optional |
| | In Layer 2 Ethernet interface view | interface interface-type interface-number dot1x port-method { macbased portbased } | Use either approach. By default, MAC-based access control applies. |

NOTE:

To use both 802.1X and portal authentication on a port, you must specify MAC-based access control. For more information about portal authentication, see the chapter “Portal configuration.”

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 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.

Follow these steps to set the maximum number of concurrent 802.1X users on a port:

| To do... | | Use the command... | Remarks |
|---|------------------------------------|---|---|
| Enter system view | | system-view | — |
| Set the maximum number of concurrent 802.1X users on a port | In system view | dot1x max-user user-number [interface interface-list] | Optional |
| | In Layer 2 Ethernet interface view | interface interface-type interface-number dot1x max-user user-number [interface interface-list] | Use either approach. By default, the maximum number of concurrent 802.1X users 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.

Follow these steps to set the maximum number of authentication request attempts:

| To do... | Use the command... | Remarks |
|--|---|--------------------------|
| Enter system view | system-view | — |
| Set the maximum number of attempts for sending an authentication request | dot1x retry <i>max-retry-value</i> | Optional 2 by default |

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.

Follow these steps to set the 802.1X timers:

| To do... | Use the command... | Remarks |
|------------------------------|---|---|
| Enter system view | system-view | — |
| Set the client timeout timer | dot1x timer supp-timeout <i>supp-timeout-value</i> | Optional The default is 30 seconds. |
| Set the server timeout timer | dot1x timer server-timeout <i>server-timeout-value</i> | Optional The default is 100 seconds. |

Configuring the online user handshake function

About 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 ensure 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

Follow these steps to configure the online user handshake function:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Set the handshake timer | dot1x timer handshake-period <i>handshake-period-value</i> | Optional The default is 15 seconds. |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Enable the online handshake function | dot1x handshake | Optional Enabled by default |
| Enable the online handshake security function | dot1x handshake secure | Optional Disabled by default |

NOTE:

- When 802.1X clients do not support exchanging handshake packets with the device, disable the online user handshake function on the device. If not, the device will tear down the connections with these online users for not receiving handshake responses.
- HP recommends that you use the iNode client software and iMC server to ensure the normal operation of the online user handshake security function.

Configuring the authentication trigger function

About 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

Follow these steps to configure the authentication trigger function on a port:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Set the username request timeout timer | dot1x timer tx-period <i>tx-period-value</i> | Optional The default is 30 seconds. |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Enable an authentication trigger function | 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.

Follow these steps to specify a mandatory authentication domain for a port:

| To do... | Use the command... | Remarks |
|--|---|--------------------------------------|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Specify a mandatory 802.1X authentication domain on the port | dot1x mandatory-domain <i>domain-name</i> | Required Not specified by default |

Enabling 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.

Follow these steps to enable the quiet timer:

| To do... | Use the command... | Remarks |
|------------------------|---|--|
| Enter system view | system-view | — |
| Enable the quiet timer | dot1x quiet-period | Required Disabled by default |
| Set the quiet timer | dot1x timer quiet-period <i>quiet-period-value</i> | 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.

Follow these steps to enable the periodic online user re-authentication function:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Set the periodic re-authentication timer | dot1x timer reauth-period <i>reauth-period-value</i> | Optional The default is 3600 seconds. |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Enable periodic online user re-authentication | dot1x re-authenticate | Required Disabled by default |

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.

NOTE:

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.

Configuring an 802.1X guest VLAN

Configuration guidelines

Follow these guidelines when configuring 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 for the voice VLAN, the default 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 re-configure the port as a tagged member in the VLAN.
- Use Table 6 when configuring multiple security features on a port.

Table 6 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 is not assigned to the MAC authentication guest VLAN. | The chapter “MAC authentication configuration” |
| 802.1X Auth-Fail VLAN on a port that performs MAC-based access control | The 802.1X Auth-Fail VLAN has a higher priority | The chapter “802.1X configuration” |
| 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. | The chapter “Port security configuration” |

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.
- 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 the *Layer 2—LAN Switching Configuration Guide*.

Configuration procedure

Follow these steps to configure an 802.1X guest VLAN:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Configure an 802.1X guest VLAN for one or more ports | In system view dot1x guest-vlan <i>guest-vlan-id</i> [interface <i>interface-list</i>] | Required Use either approach. |
| | In Layer 2 Ethernet interface <i>interface-type interface-number</i> | By default, no 802.1X guest VLAN is configured on any port. |

| To do... | Use the command... | Remarks |
|----------------|--|---------|
| interface view | dot1x guest-vlan <i>guest-vlan-id</i> | |

Configuring an Auth-Fail VLAN

Configuration guidelines

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

- Assign different IDs for the voice VLAN, the default VLAN, and the 802.1X guest 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.
- Use [Table 7](#) when configuring multiple security features on a port.

Table 7 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. | The chapter “MAC authentication configuration” |
| 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. | The chapter “Port Security configuration” |

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.
- 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 the *Layer 2—LAN Switching Configuration Guide*.

Follow these steps to configure an Auth-Fail VLAN:

| To do... | Use the command... | Remarks |
|--|---|--|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Configure the Auth-Fail VLAN on the port | dot1x auth-fail vlan <i>authfail-vlan-id</i> | Required By default, no Auth-Fail VLAN is configured. |

Displaying and maintaining 802.1X

| To do... | Use the command... | Remarks |
|--|--|------------------------|
| Display 802.1X session information, statistics, or configuration information of specified or all ports | display dot1x [sessions statistics] [interface <i>interface-list</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Clear 802.1X statistics | reset dot1x statistics [interface <i>interface-list</i>] | Available in user view |

802.1X configuration examples

802.1X authentication configuration example

Network requirements

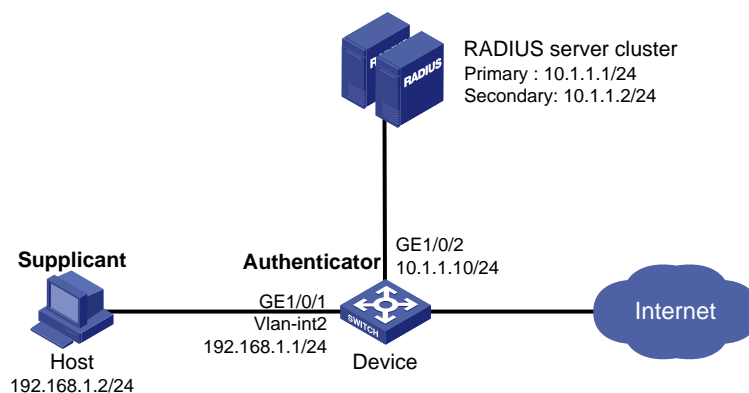
As shown in [Figure 33](#), the access device performs 802.1X authentication for users that connect to port GigabitEthernet 1/0/1. Implement MAC-based access control on the port, so the logoff of one user does not affect other online 802.1X users.

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 as the primary authentication and accounting servers, and the host at 10.1.1.2 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 33 Network diagram for 802.1X authentication configuration



Configuration procedure

NOTE:

For information about the RADIUS commands used on the access device in this example, see the [Security Command Reference](#).

1. Configure the 802.1X client. If iNode is used, do not select the **Carry version info** option in the client configuration. (Details not shown)
2. Configure the RADIUS servers and add user accounts for the 802.1X users. (Details not shown)
3. 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
```

4. 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.

5. 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
```

6. 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
```

Verification

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.

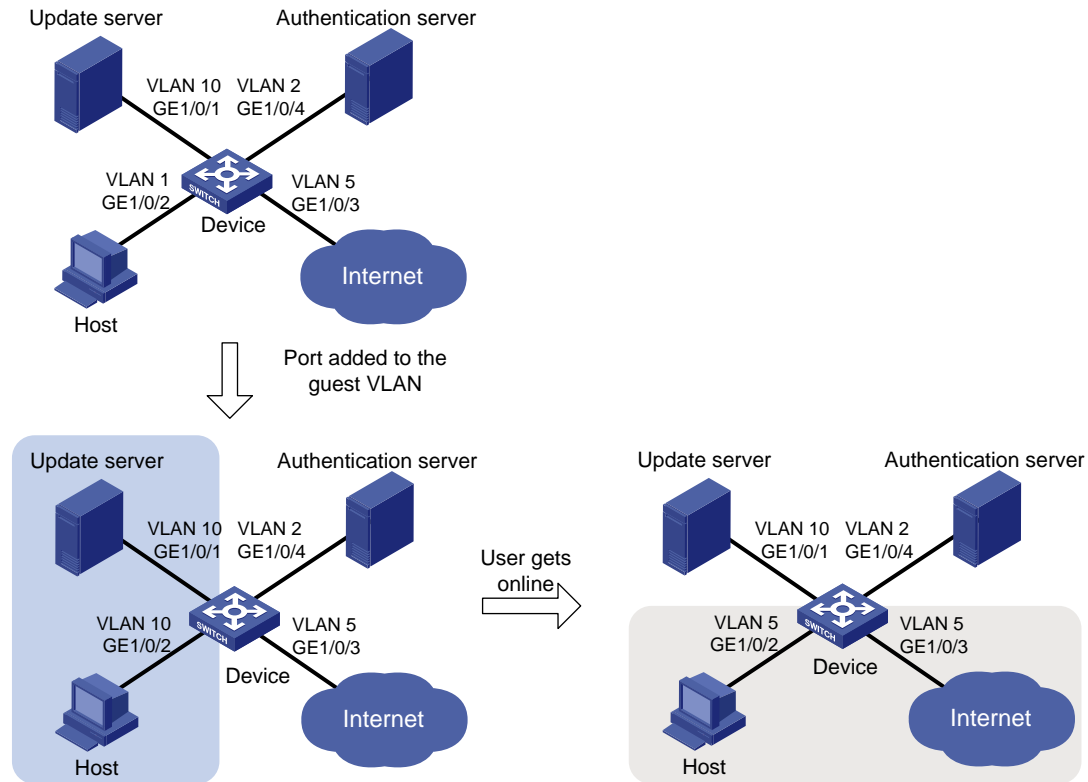
802.1X with guest VLAN and VLAN assignment configuration example

Network requirements

As shown in [Figure 34](#):

- 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 passes 802.1X authentication on GigabitEthernet 1/0/2 within a period of time (90 seconds by default), 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 host is assigned to VLAN 5 where GigabitEthernet 1/0/3 is. The host can access the Internet.

Figure 34 Network diagram for 802.1X with guest VLAN and VLAN assignment configuration



Configuration procedure

NOTE:

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 the *Security Command Reference*.

1. Configure the 802.1X client. Make sure the client is able to update its IP address after the access port is assigned to the 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] domain bbb
```

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

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

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

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

```
[Device-isp-system] 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**.

```
[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
```

Verification

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 specified 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 verify that port GigabitEthernet 1/0/2 has been added to VLAN 5.

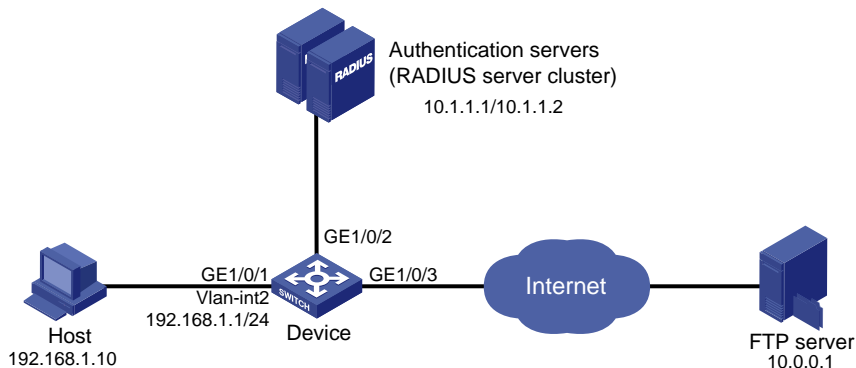
802.1X with ACL assignment configuration example

Network requirements

As shown in Figure 35, 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 802.1X users to access the FTP server.

Figure 35 Network diagram for ACL assignment



NOTE:

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 the *Security Command Reference*.

Configuration procedure

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 ACL 3000 to deny packets destined for the FTP server at 10.0.0.1.
[Device] acl number 3000
[Device-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0

# 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
```

Verification

Use the user account to pass authentication. Then ping 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),
```

The output shows that ACL 3000 is valid. You cannot access the FTP server.

EAD fast deployment configuration

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 a network that deploys EAD, 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 implementation

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 specified 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.

Configuring EAD fast deployment

Configuration prerequisites

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

Configuration procedure

Configuring 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.

Follow these steps to configure a free IP:

| To do... | Use the command... | Remarks |
|---------------------|---|---|
| Enter system view | system-view | — |
| Configure a free IP | dot1x free-ip <i>ip-address</i> { <i>mask-address</i> <i>mask-length</i> } | Required By default, no free IP is configured. |

NOTE:

When global MAC authentication, Layer-2 portal authentication, or port security is enabled, the free IP does not take effect.

Configuring the redirect URL

Follow these steps to configure a redirect URL:

| To do... | Use the command... | Remarks |
|----------------------------|------------------------------------|--|
| Enter system view | system-view | — |
| Configure the redirect URL | dot1x url <i>url-string</i> | Required By default, no redirect URL is configured. |

NOTE:

The redirect URL must be on the free IP subnet.

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.

Follow these steps to set the EAD rule timer:

| To do... | Use the command... | Remarks |
|------------------------|---|--|
| Enter system view | system-view | — |
| Set the EAD rule timer | dot1x timer ead-timeout <i>ead-timeout-value</i> | Optional The default timer is 30 minutes. |

Displaying and maintaining EAD fast deployment

| To do... | Use the command... | Remarks |
|--|--|-----------------------|
| Display 802.1X session information, statistics, or configuration information | display dot1x [sessions statistics] [interface <i>interface-list</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

EAD fast deployment configuration example

Network requirements

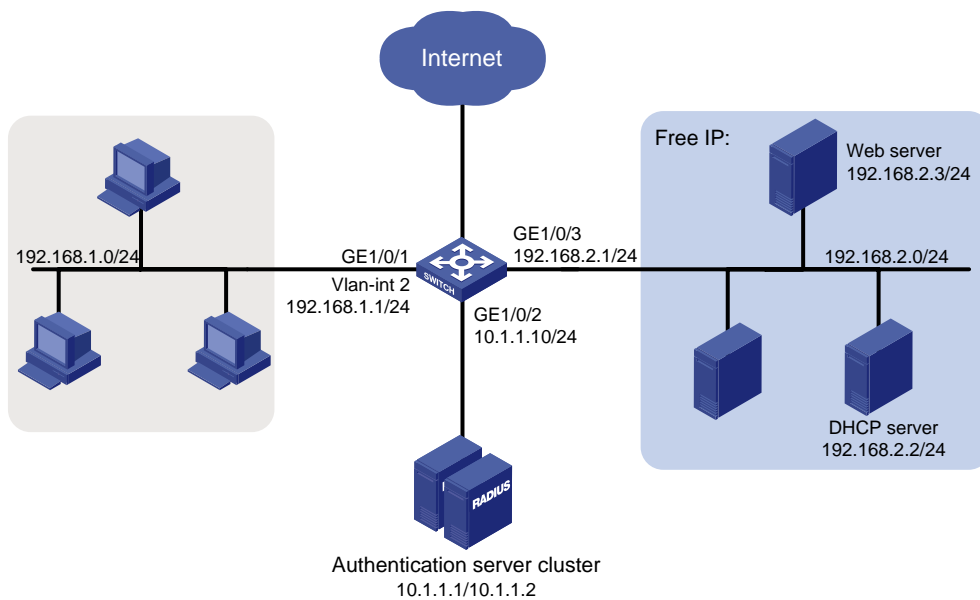
As shown in Figure 36, the hosts at the intranet 192.168.1.0/24 are attached to port GigabitEthernet 1/0/1 of the network access device, and they use DHCP to obtain IP addresses.

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 36 Network diagram for EAD fast deployment



NOTE:

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 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 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
```

2. Configure a RADIUS scheme and an ISP domain.

For more information about configuration procedure, see the chapter “802.1X configuration.”

3. Configure 802.1X.

```
# Configure the free IP.
<Device> system-view
[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
```

Verification

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.

Before passing 802.1X authentication, if a user uses a web browser to access any external website, the user is redirected to the web server, which provides the 802.1X client software download service. Enter the external website address in the address bar in the format of X.X.X.X in dotted decimal notation, for

example, 3.3.3.3 or http://3.3.3.3. The external website address should not be on the freely accessible network segment.

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 not 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

- Enter a dotted decimal IP address that is not in any free IP segment.
- Ensure that the network access device and the server are correctly configured.

MAC authentication configuration

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 it 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 the chapter “AAA configuration.”

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 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 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.

NOTE:

- 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 the port is a hybrid port with MAC-based VLAN enabled, the device maps the MAC address of each user to the VLAN assigned by the authentication server. The default VLAN of the port does not change. When a user logs off, the MAC-to-VLAN mapping for the user is removed.
-

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 when 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, it 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.

NOTE:

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.

MAC authentication configuration task list

Perform these tasks to configure MAC authentication:

| Task | Remarks |
|--|--|
| Basic configuration for MAC authentication | Configuring MAC authentication globally |
| | Configuring MAC authentication on a port |
| Specifying an authentication domain for MAC authentication users | Optional |
| Configuring a MAC authentication guest VLAN | Optional |

Basic configuration for MAC authentication

Configuration prerequisites

- 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.

NOTE:

If you are using MAC-based accounts, ensure that the username and password for each account is the same as the MAC address of the MAC authentication users.

Configuration procedure

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

Configuring MAC authentication globally

Follow these steps to configure MAC authentication globally:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|--|--|---|
| Enable MAC authentication globally | mac-authentication | Required Disabled by default |
| Configure MAC authentication timers | mac-authentication timer { offline-detect <i>offline-detect-value</i> quiet <i>quiet-value</i> server-timeout <i>server-timeout-value</i> } | Optional By default, the offline detect timer is 300 seconds, the quiet timer is 60 seconds, and the server timeout timer is 100 seconds. |
| Configure the properties of MAC authentication user accounts | mac-authentication user-name-format { fixed [account <i>name</i>] [password { cipher simple } <i>password</i>] 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, and the MAC address is hyphen separated. |

Configuring MAC authentication on a port

Follow these steps to configure MAC authentication on a port:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Enable MAC authentication for specified ports | In system view mac-authentication interface <i>interface-list</i> | Required |
| | In Layer 2 Ethernet interface view interface <i>interface-type</i> <i>interface-number</i> mac-authentication | Use either approach. Disabled by default |
| Set the maximum number of concurrent MAC authentication users allowed on a port | mac-authentication max-user <i>user-number</i> | Optional 256 by default |

NOTE:

You cannot enable MAC authentication on a link aggregation member port. If MAC authentication is enabled on a port, you cannot assign it to a link aggregation.

Specifying an authentication domain for MAC authentication users

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:

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

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

Follow these steps to specify an authentication domain for MAC authentication users:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Specify an authentication domain for MAC authentication users | mac-authentication domain <i>domain-name</i> | Required Use either approach |
| | interface <i>interface-type interface-number</i> mac-authentication domain <i>domain-name</i> | By default, no authentication domain is specified and the system default authentication domain is used for MAC authentication users. |

Configuring a MAC authentication guest VLAN

Configuration prerequisites

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.

Configuration procedure

Follow these steps to configure a MAC authentication guest VLAN:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Configure a MAC authentication guest VLAN | mac-authentication guest-vlan <i>guest-vlan-id</i> | Required By default, no MAC authentication guest VLAN is configured. You can configure only one MAC authentication guest VLAN on a port. |

Follow the guidelines in [Table 8](#) when configuring a MAC authentication guest VLAN on a port.

Table 8 Relationships of the MAC authentication guest VLAN with other security features

| Feature | Relationship description | Reference |
|--|--|---|
| MAC authentication quiet function | The MAC authentication guest VLAN function has higher priority. A user can access any resources in the guest VLAN. | 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 shut down port action of the port intrusion protection feature. | The chapter "Port security configuration" |
| 802.1X guest VLAN on a port that performs MAC-based access control | The MAC authentication guest VLAN has a lower priority. | The chapter "802.1X configuration" |

Displaying and maintaining MAC authentication

| To do... | Use the command... | Remarks |
|--|---|------------------------|
| Display the MAC authentication related information | display mac-authentication [interface <i>interface-list</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Clear the MAC authentication statistics | reset mac-authentication statistics [interface <i>interface-list</i>] | Available in user view |

MAC authentication configuration examples

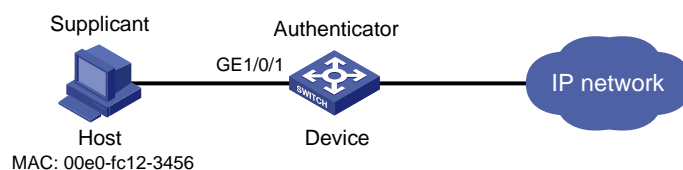
Local MAC authentication configuration example

Network requirements

In the network in [Figure 37](#), perform local MAC authentication on port GigabitEthernet 1/0/1 to control Internet access. Ensure 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 37 Network diagram for local MAC authentication



Configuration procedure

1. Configure local MAC authentication.

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**, and 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 for 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
```

2. Verify 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
```

```

Index=29 ,Username=00-e0-fc-12-34-56@aabbcc.net
MAC=00e0-fc12-3456
IP=N/A
IPv6=N/A
Total 1 connection(s) matched.

```

RADIUS-based MAC authentication configuration example

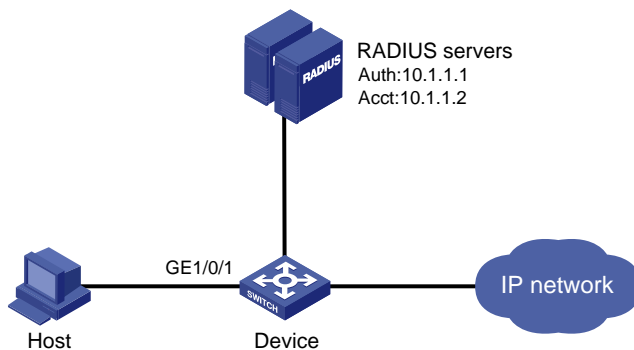
Network requirements

As shown in Figure 38, a host connects to the device through port GigabitEthernet 1/0/1. The device uses RADIUS servers for authentication, authorization, and accounting.

Perform MAC authentication on port GigabitEthernet 1/0/1 to control Internet access. Ensure 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 38 Network diagram for RADIUS-based MAC authentication



Configuration procedure

NOTE:

Ensure that the RADIUS server and the access device can reach each other. Create a shared account for MAC authentication users on the RADIUS server, and set the username **aaa** and password **123456** for the account.

1. Configure RADIUS-based MAC authentication on the device.

```
# Configure a RADIUS scheme.
```

```
<Device> system-view
```

```
[Device] radius scheme 2000
```

```
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication 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 password **123456** for the account shared by MAC authentication users.

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

2. Verify 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:123456
    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 the user passes authentication, use the **display connection** command to display the online user information.

```
<Device> display connection

Index=29 ,Username=aaa@2000
MAC=00e0-fc12-3456
IP=N/A
IPv6=N/A
Total 1 connection(s) matched.
```

ACL assignment configuration example

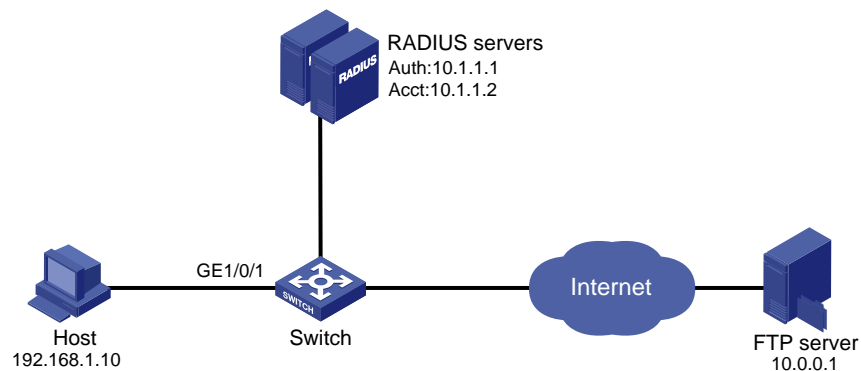
Network requirements

As shown in [Figure 39](#), a host connects to the device's port GigabitEthernet 1/0/1, and the device performs RADIUS servers for authentication, authorization, and accounting.

Perform MAC authentication on port GigabitEthernet 1/0/1 to control Internet access. Ensure 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 39 Network diagram for ACL assignment



Configuration procedure

NOTE:

Check that the RADIUS server and the access device can reach each other.

1. 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
```

2. Configure RADIUS-based MAC authentication on the device.

Configure the 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 abc
[Sysname-radius-2000] key accounting 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 users.

```
[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
```

3. 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 server-assigned ACL for the user account. (Details not shown)

4. Verify the configuration.

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

```
[Sysname-GigabitEthernet1/0/1] display connection
```

```
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.
```

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

Portal configuration

Portal overview

Introduction to portal

Portal authentication helps control access to the Internet. Portal authentication 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

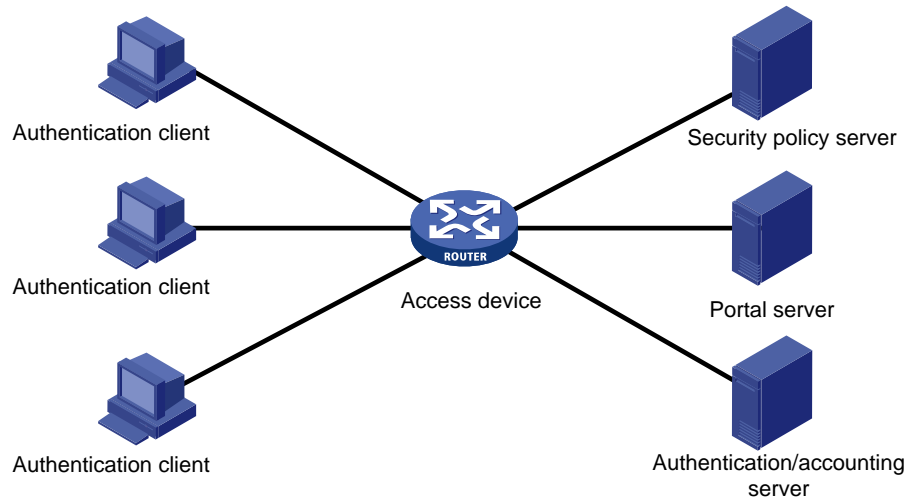
By forcing users to implement patching and anti-virus policies, extended portal functions help users to defend against viruses. The main extended functions are described as follows:

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

Portal system components

As shown in [Figure 40](#), a typical portal system consists of five basic components: authentication client, access device, portal server, authentication/accounting server, and security policy server.

Figure 40 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. The 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

An access device controls user access. It can be a switch or router that provides the following three functions:

- Redirecting all HTTP requests from unauthenticated users in authentication subnets to the portal server.
- Interacting with the portal server, security policy server and 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.

Security policy server

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

The five components 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 security policy for the user. If not, it allows the user to access the Internet. Otherwise, the client communicates with the access device and 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:

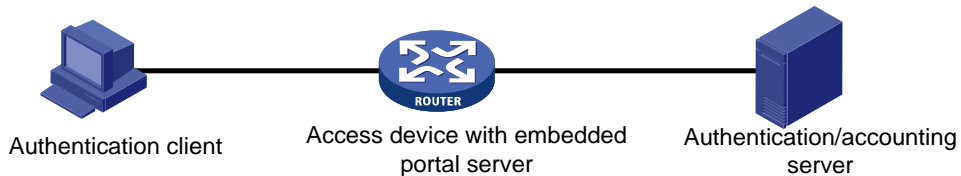
- An authentication client uses its IP address as its ID. To avoid authentication failures due to address translations, make sure that there is no Network Address Translation (NAT) device between the authentication client, access device, portal server, and authentication/accounting server when deploying portal authentication.
 - Only a RADIUS server can serve as the remote authentication/accounting server in a portal system.
 - To implement security check, the client must be the iNode client.
-

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. In this case, the portal system consists of only three components: authentication client, access device, and authentication/accounting server, as shown in Figure 41.

Figure 41 Portal system using the local portal server



NOTE:

- A portal system using the local portal server does not support extended portal functions. You do not need to configure any security policy server for it.
 - 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 completely take the place of an independent portal server.
-

Protocols used for interaction between the client and local portal server

HTTP and 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.

NOTE:

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 A5120 EI Switch Series supports only Layer 2 authentication mode.

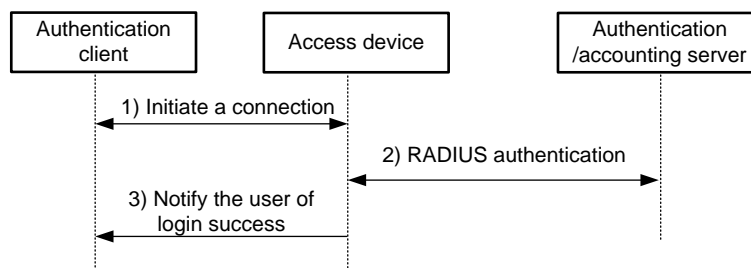
In Layer 2 authentication mode, portal authentication is enabled on an access device’s Layer 2 port that connects authentication clients, and allows only clients whose source MAC addresses pass authentication to access the external network. Now, only local portal authentication supports Layer 2 mode, where the access device serves as the local portal server to perform web authentication on clients.

In addition, Layer 2 authentication allows the authentication server to assign different VLANs according to user authentication results so that access devices can 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

Only local portal authentication supports Layer 2 mode. [Figure 42](#) illustrates the process of local Layer-2 portal authentication:

Figure 42 Local Layer-2 portal authentication process



As shown in [Figure 42](#), the local Layer-2 portal authentication process includes the following steps.

1. The portal authentication client sends an HTTP or HTTPS request. Upon receiving the HTTP request, the access device redirects it to the listening IP address of the local portal server, which then pushes a web authentication page to the authentication client. The user types the username and password on 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 which is routable to 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, which will then add the user to the authorized VLAN and generate a MAC VLAN entry. If this VLAN does not exist, the access device will first create the VLAN and then add the user to the VLAN.

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

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 MAC-based Auth-Fail VLAN (MAFV). 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 ensure 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 Layer 2 portal authentication:

| Task | Remarks | |
|--|--|----------|
| Specifying the local portal server for Layer 2 portal authentication | Required | |
| Configuring the local portal server | Customizing authentication pages | Optional |
| | Configuring the local portal server | 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 | |
| | Adding a web proxy server port number | |
| | Enabling support for portal user moving | |
| Specifying the Auth-Fail VLAN for portal authentication | Optional | |
| Specifying the auto redirection URL for authenticated portal users | 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.

Before you configure portal authentication, complete the following tasks:

- 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 are routable to 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 the chapter “AAA configuration.”
- To implement extended portal functions, install and configure iMC EAD, and ensure that the ACLs configured on the access device correspond to those specified for resources in the quarantined area and restricted resources on the security policy server respectively. For information about security policy server configuration on the access device, see the chapter “AAA configuration.”

NOTE:

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

Specifying the local portal server for Layer 2 portal authentication

Layer 2 portal authentication uses the local portal server. You need to 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 strongly recommends that you use the IP address of a loopback interface rather than a physical Layer 3 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.

Follow these steps to specify the local portal server for Layer 2 portal authentication:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Specify the listening IP address of the local portal server for Layer 2 portal authentication | portal local-server ip <i>ip-address</i> | Required 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, you need to follow the following rules when customizing authentication pages:

Rules on file names

The main authentication pages have predefined file names, which cannot be changed. The following table lists the names.

Table 9 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;">
</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, and must be saved in the specified directory of the device. 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 users passing authentication 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 logonSuccess.htm.

See the contents in gray:

```

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

```

NOTE:

- HP recommends that you use browser IE 6.0 or above on the authentication clients.
 - Ensure that 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 web site from either of the pages, the device also logs off the user.
 - If a user is using the Chrome browser, the device cannot log off the user when the user closes the logon success or online page.
-

Configuring the local portal server

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

Configuration prerequisites

Before you configure the local portal server to support HTTPS, complete the following tasks:

- Configure PKI policies, obtain the CA certificate, and apply for a local certificate. For more information, see the chapter "PKI configuration."

- Configure the SSL server policy, and specify the PKI domain to be used, which is configured in the above step. For more information, see the chapter “SSL configuration.”

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. To ensure that the local portal server uses the user-defined default authentication pages, you need to edit and save them properly. Otherwise, the system default authentication pages will be used.

Configuration procedure

Follow these steps to configure the local portal server:

| To do... | Use the command... | Remarks |
|--|---|--|
| Enter system view | system-view | — |
| 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 <i>policy-name</i> } | Required By default, the local portal server does not support any protocol. |
| Configure the welcome banner of the default authentication pages of the local portal server | portal server banner <i>banner-string</i> | Optional No welcome banner by default. |

Enabling Layer 2 portal authentication

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

Before enabling Layer 2 portal authentication, make sure that the listening IP address of the local portal server is specified.

Follow these steps to enable Layer 2 portal authentication:

| To do... | Use the command... | Remarks |
|--|---|-------------------------------------|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Enable Layer 2 portal authentication on the port | portal local-server enable | Required Not enabled by default. |

NOTE:

- To ensure normal operation of portal authentication on a Layer 2 port, HP does not recommend you to 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.

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.

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.

Follow these steps to configure a portal-free rule:

| To do... | Use the command... | Remarks |
|------------------------------|---|----------|
| Enter system view | system-view | — |
| Configure a portal-free rule | portal free-rule <i>rule-number</i> { destination { any ip { <i>ip-address</i> mask { <i>mask-length</i> <i>netmask</i> } any } } } * | Required |

NOTE:

- You cannot configure two or more portal-free rules with the same filtering criteria. Otherwise, the system prompts that the rule already exists.
- No matter whether portal authentication is enabled or not, 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.

Follow these steps to set the maximum number of online portal users allowed in the system:

| To do... | Use the command... | Remarks |
|---|--|------------------------------|
| Enter system view | system-view | — |
| Set the maximum number of online portal users | portal max-user <i>max-number</i> | Required 1000 by default. |

NOTE:

- The maximum number of online portal users that is assigned by the switch depends on the ACL resources of the switch.
- If the maximum number of online portal users specified in the command is less than that of the current online portal users, the command can be executed successfully and will not impact the online portal users, but the system will not allow new portal users to log on until the number drops down below the limit.

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.

Follow these steps to specify an authentication domain for portal users on an interface:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Enter interface view | interface <i>interface-type</i> <i>interface-number</i> | — |
| Specify an authentication domain for portal users on the interface | portal domain <i>domain-name</i> | Required By default, no authentication domain is specified for portal users. |

NOTE:

The device 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 the chapter “AAA configuration.”

Adding a web proxy server port number

NOTE:

Only Layer 2 portal authentication supports this feature.

By default, only HTTP requests from unauthenticated users to port 80 trigger portal authentication. If an unauthenticated user uses a web proxy server and the port number of the proxy server is not 80, the user's HTTP requests cannot trigger portal authentication and will be dropped. To solve this problem, configure the port numbers of the web proxy servers on the device.

If there are web servers that use non-80 port numbers on your network and users must pass portal authentication before accessing the servers, you can also add proxy web server port numbers on the device for the web servers so that HTTP requests to those web servers trigger portal authentication.

Follow these steps to add a web proxy server port number so that HTTP requests destined for this port number trigger portal authentication:

| To do... | Use the command... | Remarks |
|------------------------------------|---|---|
| Enter system view | system-view | — |
| Add a web proxy server port number | portal web-proxy port <i>port-number</i> | Required By default, no web proxy server port number is configured, and only HTTP requests to port 80 trigger portal authentication. |

NOTE:

- If the port number of a web proxy server is 80, you do not need to configure the port number of the server on the device.
 - If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover web proxy servers, you need to add the port numbers of the web proxy servers on the device, and configure portal-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.
 - For Layer 2 portal authentication, you need to add the port numbers of the web proxy servers on the device and users need to ensure that 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 will not be sent to the web proxy server.
-

Enabling support for portal user moving

NOTE:

Only Layer 2 portal authentication supports this feature.

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, 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 two 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.

Follow these steps to enable support for portal user moving:

| To do... | Use the command... | Remarks |
|---------------------------------------|------------------------------|---------------------------------|
| Enter system view | system-view | — |
| Enable support for portal user moving | portal move-mode auto | Required Disabled by default |

NOTE:

For a user with authorization information (such as authorized VLAN) configured, after the user moves from a port to another, the device tries to assign the authorization information to the new port. If the operation fails, the device deletes the user's information from the original port and re-authenticates the user on the new port.

Specifying the Auth-Fail VLAN for portal authentication

NOTE:

Only Layer 2 portal authentication supports this feature.

You can specify the Auth-Fail VLAN to be assigned to users failing portal authentication.

Before specifying the Auth-Fail VLAN, be sure to create the VLAN.

Follow these steps to specify the Auth-Fail VLAN for portal authentication:

| To do... | Use the command... | Remarks |
|--|---|--------------------------------------|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Specify the Auth-Fail VLAN for portal authentication on the port | portal auth-fail vlan <i>authfail-vlan-id</i> | Required Not specified by default |

NOTE:

- To make the Auth-Fail VLAN of portal authentication on a port take effect, you also need to enable the MAC-based VLAN function on the port. For information about MAC VLAN, see the *Layer 2—LAN Switching Configuration Guide*.
 - 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.
 - The MAC-VLAN entries generated due to portal authentication failures will not overwrite the MAC-VLAN entries already generated in other authentication modes.
-

Specifying the 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 steps to specify the auto redirection URL for authenticated portal users:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Specify the auto redirection URL for authenticated portal users | portal redirect-url <i>url-string</i> [wait-time <i>period</i>] | Required By default, a user authenticated by the local portal server is not redirected, while a user authenticated by a remote portal server is redirected to the URL the user typed in the address bar before portal authentication. |

NOTE:

The **wait-time** *period* keyword and argument combination is effective to only local 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.

Follow these steps to set the Layer 2 portal user detection interval:

| To do... | Use the command... | Remarks |
|--|---|------------------------------------|
| Enter system view | system-view | — |
| Enter interface view | interface <i>interface-type interface-number</i> | — |
| Set the Layer 2 portal user detection interval | portal offline-detect interval <i>offline-detect-interval</i> | Required 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.

Follow these steps to log off users:

| To do... | Use the command... | Remarks |
|-------------------|--|----------|
| Enter system view | system-view | — |
| Log off users | portal delete-user { <i>ip-address</i> all interface <i>interface-type interface-number</i> } | Required |

Displaying and maintaining portal

| To do... | Use the command... | Remarks |
|---|---|-----------------------|
| Display information about a portal-free rule or all portal-free rules | display portal free-rule [<i>rule-number</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display the portal configuration of a specified interface | display portal interface <i>interface-type interface-number</i> [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display configuration information about the local portal server | display portal local-server [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

| To do... | Use the command... | Remarks |
|---|--|------------------------|
| Display TCP spoofing statistics | display portal tcp-cheat statistics [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display information about portal users on a specified interface or all interfaces | display portal user { all interface <i>interface-type interface-number</i> } [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Clear TCP spoofing statistics | reset portal tcp-cheat statistics | Available in user view |

Portal configuration examples

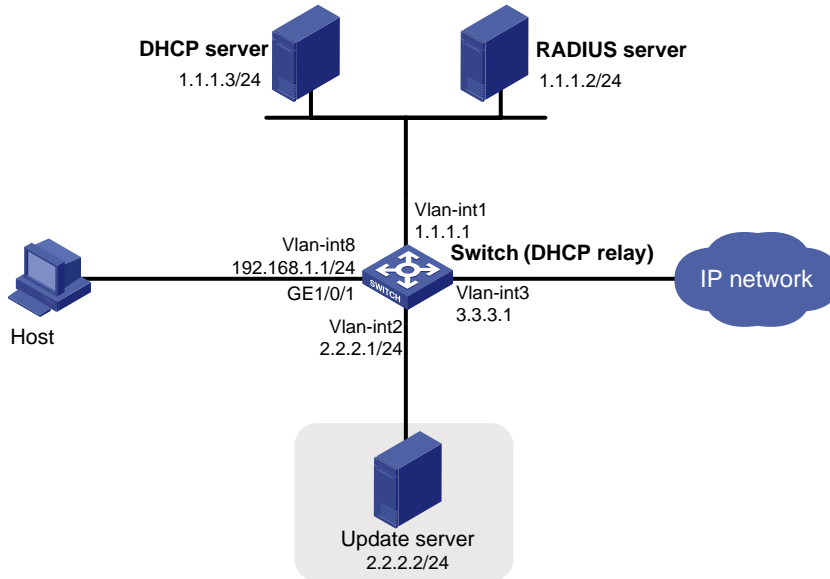
Configuring Layer 2 portal authentication

Network requirements

As shown in [Figure 43](#), 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 43 Network diagram for Layer 2 portal authentication configuration



Configuration procedures

NOTE:

- Ensure 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 need to 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 need to 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), specify the device to not assign the update server's address 2.2.2.2 to any host, specify the leases of the assigned IP addresses (set a short lease duration for each address to shorten the IP address update time in case of an authentication state change) and make sure there is a route to the host.
- As 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 the *Layer 3—IP Services Configuration Guide*.

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 the chapter "PKI configuration."

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 radius
[Switch-radius-rs1] key authentication 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 **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
```

Verification

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 access 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=2011-01-26 17:40:02 , Current=2011-01-26 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 will be 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 ensure 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

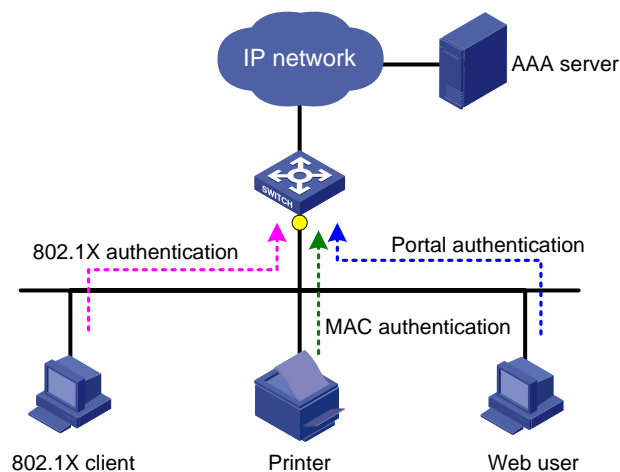
Use the **display portal server** command to display the listening port of the portal server configured on the access device and use the **portal server** command in the system view to modify it to ensure that it is the actual listening port of the portal server.

Triple authentication configuration

Triple authentication overview

The terminals in a LAN may support different authentication methods. As shown in [Figure 44](#), a printer supports only MAC authentication, a PC installed with the 802.1X client supports 802.1X authentication, and the other PC carries out portal authentication. To satisfy the different authentication requirements, the port of the access device which connects to the terminals needs to support all the three types of authentication and allow a terminal to access the network after the terminal passes one type of authentication.

Figure 44 Triple authentication network diagram



The triple authentication solution can satisfy the requirements. It is implemented by enabling portal authentication, MAC authentication, and 802.1X authentication on a Layer-2 access port. A terminal connected to that port can access the network after passing a type of authentication.

NOTE:

For more information about portal authentication, MAC authentication, and 802.1X authentication, see the chapters “Portal configuration,” “MAC authentication configuration,” and “802.1X configuration.”

Triple authentication mechanism

The three types of authentication enabled on an access port are triggered differently.

- Upon receiving an ARP or DHCP broadcast packet from a terminal for the first time, the access port performs MAC authentication on the terminal. If the terminal passes MAC authentication, no other types of authentication will be performed for it. If it fails, 802.1X or portal authentication can be triggered.
- Upon receiving an EAP packet from an 802.1X client or a thirty-party client, the access port performs only 802.1X authentication on the terminal.

- Upon receiving an HTTP packet from a terminal, the access port performs portal authentication on the terminal.

If a terminal triggers different types of authentication, the authentications are processed at the same time. A 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 authentication 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 port enabled with the three types of authentication also supports the following extended functions.

VLAN assignment

After a terminal passes authentication, the authentication server assigns a VLAN to the access port for the access terminal. The terminal can then access the network resources in the server-assigned 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.

Detection of online terminals

- You can enable an online detection timer to detect online portal clients. The timer defaults to 5 minutes, and is not configurable.
- You can enable the online handshake or periodic online user 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.

NOTE:

For more information about the extended functions, see the chapters “802.1X configuration,” “MAC authentication configuration,” and “Portal configuration.”

Configuring triple authentication

Follow these steps to configure triple authentication:

| To do... | Use the command... | Remarks |
|---------------------------------|--|----------|
| Configure 802.1X authentication | See the chapter “802.1X configuration” | Required |

| To do... | Use the command... | Remarks |
|---|--|--|
| Configure MAC authentication | See the chapter "MAC authentication configuration" | Configure at least one type of authentication. |
| Configure Layer-2 portal authentication | See the chapter "Portal configuration" | |

NOTE:

802.1X authentication must use MAC-based access control.

Triple authentication configuration examples

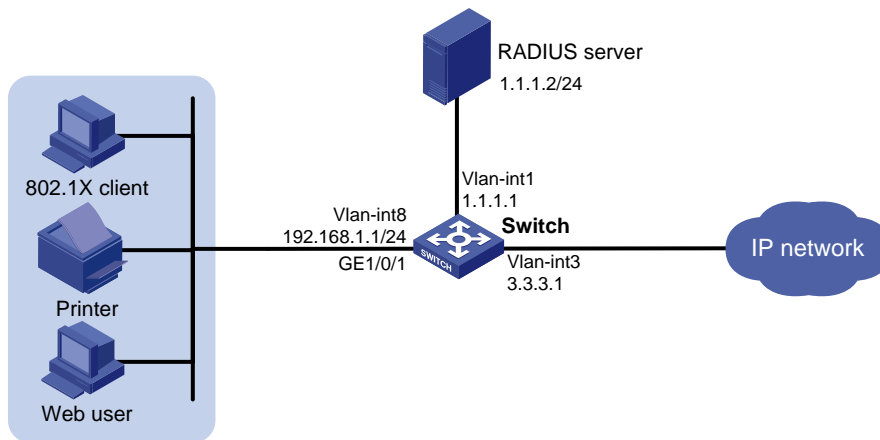
Triple authentication basic function configuration example

Network requirements

As shown in [Figure 45](#), the terminals are connected to a switch to access the IP network. It is required to 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. More specifically,

- 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 45 Network diagram for triple authentication basic configuration



Configuration procedure

NOTE:

- 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.
 - Complete the configuration on 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).
-

1. 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 12 as 4.4.4.4.

```
[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 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
```

2. 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
```

3. 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
```

4. 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
```

5. 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
```

Verification

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.
```

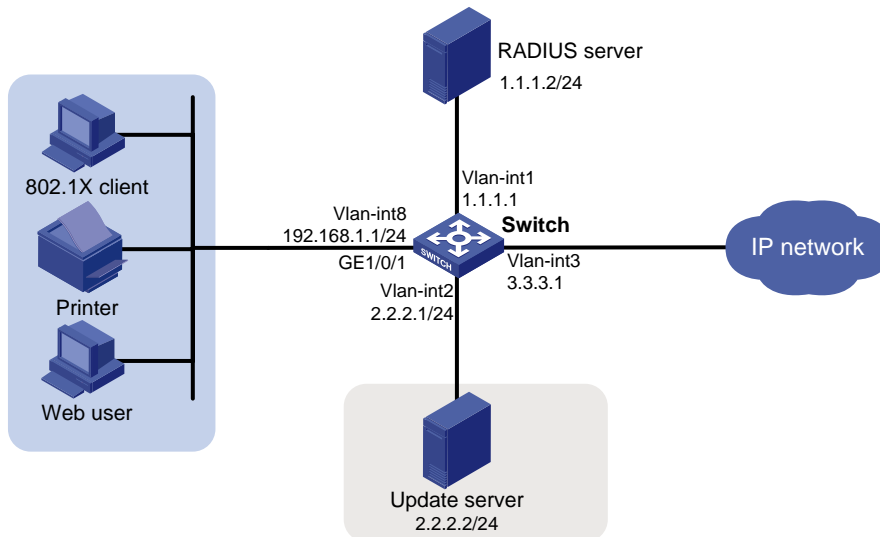

Triple authentication supporting VLAN assignment and Auth-Fail VLAN configuration example

Network requirement

As shown in Figure 46, the terminals are connected to a switch to access the IP network. It is required to 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. More specifically,

- Portal terminals request IP addresses through DHCP. They obtain 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 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 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 46 Network diagram for triple authentication supporting VLAN assignment and Auth-Fail VLAN



Configuration procedure

NOTE:

- Make sure that the terminals, the servers, and the switch can reach each other.
 - When using an external DHCP server, ensure that the terminals can get IP addresses from the server before and after authentication.
 - Complete the configuration on 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).
 - Complete the configuration of PKI domain pkidm and acquire the local and CA certificates. For more information, see the chapter “PKI configuration.”
 - 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.
-

1. 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
```

NOTE:

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
```

2. 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
```

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, 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
```

4. 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
```

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
```

Verification

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      Feb 15 2011 17:40:52  Auto:COMMITTED
3.3.3.2             0002-0002-0001      Feb 15 2011 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.

Port security configuration

Port security overview

Port security is a MAC address-based security mechanism for network access control. It is an extension to the existing 802.1X authentication and MAC authentication. It prevents access of unauthorized devices to a network by checking the source MAC address of inbound traffic and access to unauthorized devices by checking the destination MAC address of outbound traffic.

Port security enables you to control MAC address learning and authentication on ports. This enables the port to learn legal source MAC addresses.

With port security enabled, frames whose source MAC addresses cannot be learned by the device in a security mode are considered illegal; the events that users do not pass 802.1X authentication or MAC authentication are considered illegal.

Upon detection of illegal frames or events, the device takes the pre-defined action automatically. When enhancing the system security, this also greatly reduces your maintenance burden.

NOTE:

The security modes of the port security feature provide extended and combined use of 802.1X authentication and MAC authentication. They apply to scenarios that require both 802.1X authentication and MAC authentication. 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 information about 802.1X and MAC authentication, see the chapters “802.1X configuration” and “MAC authentication configuration.”

Port security features

NTK

The need to know (NTK) feature checks the destination MAC addresses in outbound frames and allows frames to be sent to only devices and hosts that have passed authentication or are using MAC addresses on the MAC address list. This prevents illegal devices from intercepting network traffic.

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 of this category use MAC authentication, 802.1X authentication, or their combinations to implement authentication.

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 an illegal frame or event is detected, the port takes the pre-defined NTK, intrusion protection, or trapping action.

Table 10 describes the port security modes and the security features.

Table 10 Port security modes

| On the port, if you want to... | Use the security mode... | Features that can be triggered | |
|---|--|----------------------------------|--------------------------|
| Turn 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. | — | |
| Control MAC address learning | autoLearn | NTK/intrusion protection | |
| | secure | | |
| Perform 802.1X authentication | userLogin | — | |
| | userLoginSecure | NTK/intrusion protection | |
| | userLoginSecureExt | | |
| | userLoginWithOUI | | |
| Perform MAC authentication | macAddressWithRadius | NTK/intrusion protection | |
| Perform a combination of MAC authentication and 802.1X authentication | Or | macAddressOrUserLoginSecure | NTK/intrusion protection |
| | | macAddressOrUserLoginSecureExt | |
| | Else | macAddressElseUserLoginSecure | |
| | | macAddressElseUserLoginSecureExt | |

 **TIP:**

These security mode naming rules may help you remember the modes:

- **userLogin** specifies 802.1X authentication and port-based access control.
- **macAddress** specifies MAC address authentication.
- **Else** specifies that the authentication method before **Else** is applied first. If the authentication fails, whether to turn to the authentication method following **Else** depends on the protocol type of the authentication request.
- In a security mode with **Or**, the authentication method to be used depends on the protocol type of the authentication request.
- **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.

Control MAC address learning

1. 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.

In addition, you can configure MAC addresses manually by using the **mac-address dynamic** and **mac-address static** commands for a port in autoLearn mode.

When the number of secure MAC addresses reaches the upper limit, the port transitions to secure mode.

On a port operating in autoLearn mode, the dynamic MAC address learning function in MAC address management is disabled.

2. secure

MAC address learning is disabled on a port in secure mode. You can configure MAC addresses by using the **mac-address static** and **mac-address dynamic** commands.

A port in secure mode allows only frames sourced from secure MAC addresses and MAC addresses manually configured to pass.

Perform 802.1X authentication

1. 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.

2. 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.

3. userLoginSecureExt

This mode is similar to the userLoginSecure mode except that this mode supports multiple online 802.1X users.

4. 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 specified 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.

Perform MAC authentication

macAddressWithRadius: A port in this mode performs MAC authentication and services multiple users.

Perform a combination of MAC authentication and 802.1X authentication

1. 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.

2. macAddressOrUserLoginSecureExt

This mode is similar to the macAddressOrUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users.

3. 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 non-802.1X frames, a port in this mode performs only MAC authentication. For 802.1X frames, it performs MAC authentication and then, if the authentication fails, 802.1X authentication.

4. 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:

- The maximum number of users a port supports equals the maximum number of secure MAC addresses or the maximum number of authenticated users the security mode supports, whichever is smaller.
 - For more information about configuring MAC address table entries, see the *Layer 2—LAN Switching Command Reference*.
-

Support for 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 the chapter “802.1X configuration.”
 - 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 the chapter “MAC authentication configuration.”
-

NOTE:

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.

Port security configuration task list

Complete the following tasks to configure port security:

| Task | Remarks | |
|--|----------------------------------|---|
| Enabling port security | Required | |
| Setting the maximum number of secure MAC addresses | Optional | |
| Setting the port security mode | Required | |
| Configuring port security features | Configuring NTK | Optional |
| | Configuring intrusion protection | Configure one or more features as required. |
| | Configuring port security traps | |
| Configuring secure MAC addresses | Optional | |

| Task | Remarks |
|--|----------|
| Ignoring authorization information from the server | Optional |

Enabling port security

Configuration prerequisites

Disable 802.1X and MAC authentication globally.

Configuration procedure

Follow these steps to enable port security:

| To do... | Use the command... | Remarks |
|----------------------|-----------------------------|----------------------------------|
| Enter system view | system-view | — |
| Enable port security | port-security enable | Required Disabled by default. |

- Enabling port security resets the following configurations on a port to the bracketed defaults. Then, values of these configurations cannot be changed manually; the system will adjust them based on the port security mode automatically:
 - 802.1X (**disabled**), port access control method (**macbased**), and port authorization mode (**auto**)
 - MAC authentication (**disabled**)
- Disabling port security resets the following configurations on a port to the bracketed defaults:
 - Port security mode (**noRestrictions**)
 - 802.1X (**disabled**), port access control method (**macbased**), and port authorization mode (**auto**)
 - MAC authentication (**disabled**)
- Port security cannot be disabled when a user is present on a port.

NOTE:

- For more information about 802.1X configuration, see the chapter “802.1X configuration.”
- For more information about MAC authentication configuration, see the chapter “MAC authentication configuration.”

Setting the maximum number of secure MAC addresses

The maximum number of users a port supports in a port security mode is determined by the maximum number of secure MAC addresses or the maximum number of authenticated users that the security mode supports, whichever is smaller.

By setting the maximum number of MAC addresses allowed on a port, you can implement the following control:

- Control the number of secure MAC addresses that a port can learn for port security.
- Control the maximum number of users who are allowed to access the network through the port.

Follow these steps to set the maximum number of secure MAC addresses allowed on a port:

| To do... | Use the command... | Remarks |
|--|---|------------------------------------|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Set the maximum number of secure MAC addresses allowed on a port | port-security max-mac-count <i>count-value</i> | Required Not limited by default |

NOTE:

This configuration is independent of the MAC learning limit described in MAC address table configuration in the *Layer 2—LAN Switching Configuration Guide*.

Setting the port security mode

Configuration prerequisites

Before you set a port security mode for a port, complete the following tasks:

- Disable 802.1X and MAC authentication.
- Set the port to perform MAC-based access control, and set the port authorization mode to **auto**.
- Check the port does not belong to any aggregation group.

The requirements above must be all met. Otherwise, an error message appears when you set a security mode on the port. On the other hand, after setting a port security mode on a port, you cannot change any of the configurations above.

- Before you configure the port to operate in autolearn mode, set the maximum number of secure MAC addresses allowed on a port.

NOTE:

- With port security disabled, you can configure a port security mode, but your configuration does not take effect.
- You cannot change the port security mode of a port with users online.

Configuration procedure

Follow these steps to enable any other port security mode:

| To do... | Use the command... | Remarks |
|--|---|--|
| Enter system view | system-view | — |
| Set an OUI value for user authentication | port-security oui <i>oui-value index index-value</i> | Optional Not configured by default. The command is required for the userlogin-withoui mode. |

| To do... | Use the command... | Remarks |
|---------------------------------------|--|---|
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| 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 } | Required By default, a port operates in noRestrictions mode. |

NOTE:

- When a port operates in autoLearn mode, the maximum number of secure MAC addresses cannot be changed.
- An OUI, as defined by the IEEE, is the first 24 bits of the MAC address, which uniquely identifies a device vendor.
- You can configure multiple OUI values. However, a port in userLoginWithOUI mode allows only one 802.1X user and one user whose MAC address contains a specified OUI to pass authentication at the same time.
- After enabling port security, you can change the port security mode of a port only when the port is operating in noRestrictions mode, the default mode. To change the port security mode for a port in any other mode, use the **undo port-security port-mode** command to restore the default port security mode first.

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.

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.

Follow these steps to configure the NTK feature:

| To do... | Use the command... | Remarks |
|---------------------------------------|---|---------|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |

| To do... | Use the command... | Remarks |
|---------------------------|--|--|
| Configure the NTK feature | port-security ntk-mode { ntk-withbroadcasts ntk-withmulticasts ntkonly } | Required By default, NTK is disabled on a port and all frames are allowed to be sent. |

NOTE:

Support for the NTK feature depends on the port security mode.

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 specified period of time. The period can be configured with the **port-security timer disableport** command.

Follow these steps to configure the intrusion protection feature:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Configure the intrusion protection feature | port-security intrusion-mode { blockmac disableport disableport-temporarily } | Required By default, intrusion protection is disabled. |
| Return to system view | quit | — |
| Set the silence timeout period during which a port remains disabled | port-security timer disableport <i>time-value</i> | Optional 20 seconds by default |

NOTE:

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.

Configuring 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/successful authentication/802.1X user logoff.

- **ralmlogfailure/ralmlogon/ralmlogoff**—MAC authentication failure/MAC authentication user logon/MAC authentication user logoff.
- **intrusion**—Detection of illegal frames.

Follow these steps to enable port security traps:

| To do... | Use the command... | Remarks |
|----------------------------|---|---|
| Enter system view | system-view | — |
| Enable port security traps | port-security trap { addresslearned dot1xlogfailure dot1xlogoff dot1xlogon intrusion ralmlogfailure ralmlogoff ralmlogon } | Required By default, port security traps are disabled. |

Configuring secure MAC addresses

Secure MAC addresses are MAC addresses configured or learned in autoLearn mode. They can survive link down/up events, and once saved, can survive a device reboot. You can bind a MAC address to only one port in a VLAN.

Secure MAC addresses fall into static secure MAC addresses and sticky MAC addresses.

Static secure MAC addresses are manually configured at the command line or in the MIB in autoLearn mode. No aging mechanism is available for this type of MAC address. They never age out unless you manually remove them, change the port security mode, or disable the port security feature.

Sticky MAC addresses include dynamic secure MAC addresses manually configured, at the command line interface or in the MIB, and dynamic secure MAC addresses learned by a port in autoLearn mode. These MAC addresses are sticky because unlike normal dynamic MAC addresses, they can survive link down/up events, and once saved, can survive a device reboot.

By default, sticky MAC addresses do not age out. You can use the **port-security timer autolearn aging** command to set an aging timer for sticky MAC addresses. When the timer expires, the sticky MAC addresses are removed. This aging mechanism prevents the unauthorized use of a sticky MAC address when the authorized user is offline, and removes outdated secure MAC addresses so new secure MAC addresses can be learned.

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 with the **mac-address dynamic** or **mac-address static** command to pass through.

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

Follow these steps to configure a secure MAC address:

| To do... | Use the command... | Remarks |
|--------------------------------|---|--|
| Enter system view | system-view | — |
| Set the sticky MAC aging timer | port-security timer autorelearn aging <i>time-value</i> | Optional By default, sticky MAC addresses do not 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. |
| Configure a secure MAC address | In system view port-security mac-address security [sticky] <i>mac-address interface interface-type interface-number vlan vlan-id</i> | Required Use either approach |
| | In Layer 2 Ethernet interface view interface <i>interface-type interface-number</i> port-security mac-address security [sticky] <i>mac-address vlan vlan-id</i> | No secure MAC address is configured by default. |

Ignoring authorization information from the server

The authorization information is delivered by the RADIUS server to the device after an 802.1X user or MAC authenticated user passes RADIUS authentication. You can configure a port to ignore the authorization information from the RADIUS server.

Follow these steps to configure a port to ignore the authorization information from the RADIUS server:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Ignore the authorization information from the RADIUS server | port-security authorization ignore | Required By default, a port uses the authorization information from the RADIUS server. |

Displaying and maintaining port security

| To do... | Use the command... | Remarks |
|---|--|-----------------------|
| Display port security configuration information, operation information, and statistics about one or more ports or all ports | display port-security [interface <i>interface-list</i>] [[{ begin exclude include } <i>regular-expression</i>] | Available in any view |

| To do... | Use the command... | Remarks |
|---|--|-----------------------|
| Display information about secure MAC addresses | display port-security mac-address security [interface <i>interface-type interface-number</i>] [vlan <i>vlan-id</i>] [count] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display information about blocked MAC addresses | display port-security mac-address block [interface <i>interface-type interface-number</i>] [vlan <i>vlan-id</i>] [count] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

Port security configuration examples

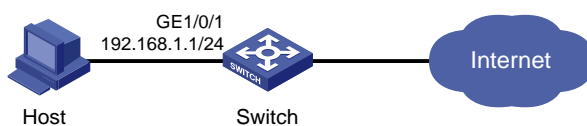
Configuring the autoLearn mode

Network requirements

Configure port GigabitEthernet 1/0/1 on the switch:

- Allow up to 64 users on the port without authentication.
- Permit the port to learn and add the MAC addresses as sticky MAC address, 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 is triggered and the port is disabled and stays silent for 30 seconds.

Figure 47 Network diagram for configuring the autoLearn mode



Configuration procedure

1. Configure port security.

Enable port security.

```
<Switch> system-view
[Switch] port-security enable
```

Set the sticky MAC aging timer to 30 minutes.

```
[Switch] port-security timer autolearn aging 30
```

Enable port security traps for intrusion protection.

```
[Switch] port-security trap intrusion
[Switch] interface gigabitethernet 1/0/1
```

Set the maximum number of secure MAC addresses allowed on the port to 64.

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

Set the port security mode to autoLearn.


```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Configure the port to be silent for 30 seconds after the intrusion protection feature is triggered.

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

```
[Switch-GigabitEthernet1/0/1] quit
```

```
[Switch] port-security timer disableport 30
```

2. Verify the configuration.

After completing the configurations, use the following command to view the port security configuration information:

```
<Switch> 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
```

As shown in the output, the maximum number of secure MAC addresses allowed on the port is 64, the port security mode is autoLearn, the port security traps for intrusion protection is enabled, and the intrusion protection action is to disable the port (DisablePortTemporarily) for 30 seconds.

You can also use the command above repeatedly to track the number of MAC addresses learned by the port, or use the **display this** command in interface view to display the secure MAC addresses learned:

```
<Switch> system-view
```

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-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
```

```
#
```

Issuing the **display port-security interface** command after the number of MAC addresses learned by the port reaches 64, you will 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 will see traps:

```
#Jan 14 10:39:47:135 2011 Switch PORTSEC/4/VIOLATION:TraphpSecureViolation
```

```
An intrusion occurs!
```

```
IfIndex: 9437185
```

```
Port: 9437185
MAC Addr: 00:02:00:00:00:32
VLAN ID: 1
IfAdminStatus: 1
```

In addition, you will see that the port security feature has disabled the port if you issue the following command:

```
[Switch-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: 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.

```
[Switch-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
.....
```

If you manually delete several secure MAC addresses, the port security mode of the port will be restored to autolearn, and the port will be able to learn MAC addresses again.

Configuring the userLoginWithOUI mode

Network requirements

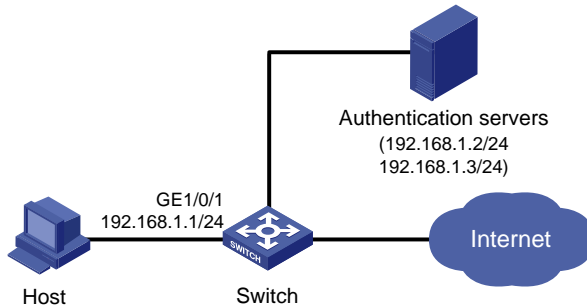
As shown in [Figure 48](#), a client is connected to the switch through port GigabitEthernet 1/0/1. The switch authenticates the client with a RADIUS server. If the authentication succeeds, the client is authorized to access the Internet.

- 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 switch 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 switch 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 48 Network diagram for configuring the userLoginWithOUI mode



Configuration procedure

NOTE:

- The following configuration steps cover some AAA/RADIUS configuration commands. For details about the commands, see the chapter “AAA configuration commands.”
 - Configurations on the host and RADIUS servers are not shown.
-

1. Configure the RADIUS protocol.

Configure a RADIUS scheme named **radsun**.

```
<Switch> system-view
[Switch] radius scheme radsun
[Switch-radius-radsun] primary authentication 192.168.1.2
[Switch-radius-radsun] primary accounting 192.168.1.3
[Switch-radius-radsun] secondary authentication 192.168.1.3
[Switch-radius-radsun] secondary accounting 192.168.1.2
[Switch-radius-radsun] key authentication name
[Switch-radius-radsun] key accounting money
[Switch-radius-radsun] timer response-timeout 5
[Switch-radius-radsun] retry 5
[Switch-radius-radsun] timer realtime-accounting 15
[Switch-radius-radsun] user-name-format without-domain
[Switch-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.

```
[Switch] domain sun
[Switch-isp-sun] authentication default radius-scheme radsun
[Switch-isp-sun] authorization default radius-scheme radsun
[Switch-isp-sun] accounting default radius-scheme radsun
[Switch-isp-sun] access-limit enable 30
[Switch-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.)

```
[Switch] dot1x authentication-method chap
```

3. Configure port security.

Enable port security.

```
[Switch] port-security enable
```

Add five OUI values.

```
[Switch] port-security oui 1234-0100-1111 index 1
[Switch] port-security oui 1234-0200-1111 index 2
[Switch] port-security oui 1234-0300-1111 index 3
[Switch] port-security oui 1234-0400-1111 index 4
[Switch] port-security oui 1234-0500-1111 index 5
[Switch] interface gigabitethernet 1/0/1
```

Set the port security mode to userLoginWithOUI.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
```

4. Verify the configuration.

After completing the configurations, you can use the following command to view the configuration information of the RADIUS scheme named **radsun**:

```
<Switch> 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
  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
  Second Acct Server:
    IP: 192.168.1.2                        Port: 1813   State: active
    Encryption Key : N/A
  Auth Server Encryption Key : name
  Acct Server Encryption Key : money
  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
```

Use the following command to view the configuration information of the ISP domain named **sun**:

```
<Switch> display domain sun
  Domain : sun
  State : Active
  Access-limit : 30
```

```
Accounting method : Required
Default authentication scheme      : radius:radius
Default authorization scheme      : radius:radius
Default accounting scheme         : radius:radius
Domain User Template:
Idle-cut : Disabled
Self-service : Disabled
Authorization attributes:
```

Use the following command to view the port security configuration information:

```
<Switch> 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
```

After an 802.1X user gets online, you can see that the number of secure MAC addresses stored is 1. You can also use the following command to view information about 802.1X:

```
<Switch> 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
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. You can use the following command to view the related information:

```
<Switch> 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 48](#), a client is connected to the switch through GigabitEthernet 1/0/1. The switch 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 switch:

- 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.
- Set fixed username and password for MAC authentication. 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

NOTE:

Configurations on the host and RADIUS servers are not shown.

1. Configure the RADIUS protocol.

The required RADIUS authentication/accounting configurations and ISP domain configurations are the same as those in [Configuring the userLoginWithOUI mode](#).

2. Configure port security.

Enable port security.

```
<Switch> system-view
[Switch] port-security enable
```

Configure a MAC authentication user, setting the username and password to aaa and 123456 respectively.

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

Specify ISP domain **sun** for MAC authentication.

```
[Switch] mac-authentication domain sun
```

Set the 802.1X authentication method to CHAP. (This configuration is optional. By default, the authentication method is CHAP for 802.1X.)

```
[Switch] dot1x authentication-method chap
```

Set the maximum number of secure MAC addresses allowed on the port to 64.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

Set the port security mode to macAddressElseUserLoginSecure.

```
[Switch-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

Set the NTK mode of the port to ntkonly.

```
[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

3. Verify the configuration.

After completing the configurations, you can use the following command to view the port security configuration information:

```
<Switch> display port-security interface gigabitethernet 1/0/1
Equipment port-security is enabled
Trap is disabled
AutoLearn aging time is 30 minutes
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
```

Use the following command to view MAC authentication information:

```
<Switch> display mac-authentication interface gigabitethernet 1/0/1
MAC address authentication is enabled.
User name format is fixed account
Fixed username:aaa
Fixed password:123456
    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 |

Use the following command to view 802.1X authentication information:

```
<Switch> 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
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, as NTK is enabled, frames with unknown destination MAC addresses, multicast addresses, and broadcast addresses should be discarded.

Troubleshooting port security

Cannot set the port security mode

Symptom

Cannot set the port security mode.

```
[Switch-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.

```
[Switch-GigabitEthernet1/0/1] undo port-security port-mode
```

```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Cannot configure secure MAC addresses

Symptom

Cannot configure secure MAC addresses.

```
[Switch-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.

```
[Switch-GigabitEthernet1/0/1] undo port-security port-mode
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
[Switch-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.

```
[Switch-GigabitEthernet1/0/1] 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.

```
[Switch-GigabitEthernet1/0/1] quit
[Switch] cut connection interface gigabitethernet 1/0/1
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] undo port-security port-mode
```

User profile configuration

User profile overview

A user profile provides a configuration template to save predefined configurations, such as a Quality of Service (QoS) policy. Different user profiles are applicable to different application scenarios.

The user profile supports working with 802.1X, MAC and portal authentications. It is capable of restricting authenticated users' behaviors. After the authentication server verifies a user, it sends the device the name of the user profile that is associated with the user. Then the device applies the configurations in the user profile if the profile is enabled, and allows user access based on all valid configurations. If the user profile is not enabled, the device denies the user access. After the user logs out, the device automatically disables the configurations in the user profile, and the restrictions on the users are removed.

Without user profiles, service applications are based on interface, VLAN, or globally, and a policy applies to any user that accesses the interface, or VLAN, or device. If a user moves between ports to access a device, to restrict the user behavior, you must remove the policy from the previous port and then configure the same policy on the port that the user currently uses. The configuration task is tedious and error prone.

User profiles provide flexible user-based service applications because a user profile is associated with a target user. Every time the user accesses the device, the device automatically applies the configurations in the associated user profile.

User profile configuration task list

Complete the following tasks to configure a user profile:

| Task | Remarks |
|--|----------|
| Creating a user profile | Required |
| Configuring a user profile | Required |
| Enabling a user profile | Required |

Creating a user profile

Configuration prerequisites

Before you create a user profile, complete the following tasks:

- Configure authentication parameters on the device.
- Perform configurations on the client, the access device, and the authentication server, for example, username, password, authentication scheme, domain, and binding a user profile with a user.

Creating a user profile

Follow these steps to create a user profile:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Create a user profile, and enter its view | user-profile <i>profile-name</i> | Required You can use the command to enter the view of an existing user profile. |

Configuring a user profile

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.

Follow these steps to configure user profile:

| To do... | Use the command... | Remarks |
|-------------------------|--|--|
| Enter system view | system-view | — |
| Enter user profile view | user-profile <i>profile-name</i> | Required |
| Apply the QoS policy | qos apply policy <i>policy-name</i> { inbound outbound } | Required 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). |

NOTE:

- If a user profile is enabled but not used by any online user, you can edit only the content of the ACL that is referenced by the QoS policy in the profile. If the user profile is being used by online users, you cannot edit any configuration in the QoS policy.
- 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.

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.

Follow these steps to enable a user profile:

| To do... | Use the command... | Remarks |
|-----------------------|---|--|
| Enter system view | system-view | — |
| Enable a user profile | user-profile <i>profile-name</i> enable | Required A user profile is disabled by default. |

NOTE:

- 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.
-

Displaying and maintaining user profile

| To do... | Use the command... | Remarks |
|---|--|-----------------------|
| Display information about all the created user profiles | display user-profile [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

Password control configuration

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.

1. 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.

2. 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 for users of the manage level. For information about user levels, see the *Fundamentals Configuration Guide*.
 - This function is not effective for a user who is prompted to change the password at the first login or a user whose password has just been aged out.
-

3. 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.

4. 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 expiry time and provides a choice for the user to change the password. If the user provides a new, qualified password, 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 present password.

NOTE:

Telnet, SSH, and terminal users can change their passwords by themselves. FTP users, on the contrary, can only have their passwords changed by the administrator.

5. Login with an expired password

You can allow a user to log in a certain number of times within a specified 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.

6. 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 used ones to see whether it was used before and, if so, 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.

7. 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 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 blacklist manually.
- Allowing the user to try continuously and removing the user from the 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 blacklist.

NOTE:

- A blacklist can contain up to 1024 entries.
 - A login attempt using a wrong username will undoubtedly fail but the username will not be added into the blacklist.
 - Users failing web authentication are not blacklisted. Users accessing the system through the Console or AUX interface are not blacklisted either, because the system is unable to obtain the IP addresses of these users and these users are privileged and relatively secure to the system.
-

8. Password composition checking

A password can be a combination of characters from the following four categories:

- Uppercase letters A to Z
- Lowercase letters a to z
- Digits 0 to 9
- 32 special characters including blank space and ~`!@#\$%^&*()_+={}|[]\:'<>.,/.

Depending on the system security requirements, you can set the minimum number of categories a password must contain and the minimum number of characters of each category.

Password combination has four levels: 1, 2, 3, and 4, each representing the number of categories that a password must at least contain. Level 1 means that a password must contain characters of one category, level 2 at least two categories, and so on.

When a user sets or changes the password, the system checks if the password satisfies the composition requirement. If not, the system displays an error message.

9. 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 ensure 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 not qualified, 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 unqualified.
- No character of the password is repeated three or more times consecutively. For example, password a111 is not qualified.

10. Password display in the form of a string of *

For the sake of security, the password a user enters is displayed in the form of a string of *.

11. 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.

12. 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.

13. Logging

The system logs all successful password changing events and user blacklisting events due to login failures.

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 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 |

| Task | Remarks |
|---|----------|
| 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. Only after the password control feature is enabled globally, can password control configurations take effect.
2. Enable password control functions. Some password control functions need to be enabled individually after the password control feature is enabled globally. These functions include:
 - Password aging
 - Minimum password length
 - Password history
 - Password composition checking

You must enable a function for its relevant configurations to take effect.

Follow these steps to enable password control:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Enable the password control feature | password-control enable | Required Disabled by default |
| 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. |

NOTE:

After global password control is enabled, local user passwords configured on the device are not displayed when you use the corresponding display command.

Setting global password control parameters

Follow these steps to set global password control parameters:

| To do... | Use the command... | Remarks |
|-----------------------------|---|--------------------------------|
| Enter system view | system-view | — |
| Set the password aging time | password-control aging <i>aging-time</i> | Optional 90 days by default |

| To do... | Use the command... | Remarks |
|--|---|---|
| Set the minimum password update interval | password-control password update interval <i>interval</i> | Optional 24 hours by default |
| Set the minimum password length | password-control length <i>length</i> | Optional 10 characters by default |
| Configure the password composition policy | password-control composition type-number <i>policy-type</i> [type-length <i>type-length</i>] | Optional By default, the minimum number of password composition types is 1 and the minimum number of characters of a password composition type is 1 too. |
| 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. |
| Set the maximum number of history password records for each user | password-control history <i>max-record-num</i> | Optional 4 by default |
| 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 <i>login-times</i> [exceed { lock unlock lock-time <i>time</i> unlock }] | 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. |
| Set the number of days during which the user is warned of the pending password expiration | password-control alert-before-expire <i>alert-time</i> | Optional 7 days by default |
| 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 <i>delay times times</i> | Optional By default, a user can log in three times within 30 days after the password expires. |
| Set the authentication timeout time | password-control authentication-timeout <i>authentication-timeout</i> | Optional 60 seconds by default |
| Set the maximum account idle time | password-control login idle-time <i>idle-time</i> | Optional 90 days by default |

△ CAUTION:

The specified action to be taken after a user fails to log in for the specified number of attempts takes effect immediately, and can affect the users already in the blacklist. Other configurations take effect only for users logging in later and passwords configured later.

Setting user group password control parameters

Follow these steps to set password control parameters for a user group:

| To do... | Use the command... | Remarks |
|--|--|--|
| Enter system view | system-view | — |
| Create a user group and enter user group view | user-group <i>group-name</i> | — |
| Configure the password aging time for the user group | password-control aging <i>aging-time</i> | Optional By default, the password aging time configured in system view is used. |
| Configure the minimum password length for the user group | password-control length <i>length</i> | Optional By default, the minimum password length configured in system view is used. |
| Configure the password composition policy for the user group | password-control composition type-number <i>type-number</i> [type-length <i>type-length</i>] | Optional By default, the password composition policy configured in system view is used. |

Setting local user password control parameters

Follow these steps to set password control parameters for a local user:

| To do... | Use the command... | Remarks |
|--|--|---|
| Enter system view | system-view | — |
| Create a local user and enter local user view | local-user <i>user-name</i> | — |
| Configure the password aging time for the local user | password-control aging <i>aging-time</i> | Optional By default, the setting for the user group to which the local user belongs is used; if no aging time is configured for the user group, the setting in system view is used. |
| Configure the minimum password length for the local user | password-control length <i>length</i> | Optional By default, the setting for the user group to which the local user belongs is used; if no minimum password length is configured for the user group, the setting in system view is used. |
| Configure the password composition policy for the local user | password-control composition type-number <i>type-number</i> [type-length <i>type-length</i>] | Optional By default, the settings for the user group to which the local user belongs are used; if no password composition policy is configured for the user group, the settings in system view are used. |

Setting super password control parameters

NOTE:

- 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 details on super passwords, see the *Fundamentals Configuration Guide*.

Follow these steps to set super password control parameters:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Set the password aging time for super passwords | password-control super aging aging-time | Optional 90 days by default |
| Configure the minimum length for super passwords | password-control super length length | Optional 10 characters by default |
| Configure the password composition policy for super passwords | password-control super composition type-number type-number [type-length type-length] | Optional By default, the minimum number of password composition types is 1 and the minimum number of characters of a password composition type is 1 too. |

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.

Follow these steps to set a password for a local user in interactive mode:

| To do... | Use the command... | Remarks |
|---|-----------------------------|----------|
| Enter system view | system-view | — |
| Create a local user and enter local user view | local-user user-name | — |
| Set the password for the local user in interactive mode | password | Required |

Displaying and maintaining password control

| To do... | Use the command... | Remarks |
|--|--|-----------------------|
| Display password control configuration information | display password-control [super] [{ begin exclude include } regular-expression] | Available in any view |

| To do... | Use the command... | Remarks |
|---|--|------------------------|
| Display information about users blacklisted due to authentication failure | display password-control blacklist [user-name <i>name</i> ip <i>ipv4-address</i> ipv6 <i>ipv6-address</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Delete users from the blacklist | reset password-control blacklist [user-name <i>name</i>] | Available in user view |
| Clear history password records | reset password-control history-record [user-name <i>name</i> super [level <i>level</i>]] | Available in user view |

NOTE:

The **reset password-control history-record** command can delete the history password records of one or all users even when the password history function is disabled.

Password control configuration example

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
# Set the minimum number of composition types for super passwords to 3 and the minimum number of
characters of each composition type to 5.
[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
# Set the minimum number of password composition types to 2 and the minimum number of characters of
each password composition type to 5 for the local user.
[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

```

Verification

```

# 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 the 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 day(s))
Password-Length:                   Enabled (12 characters)
Password-Composition:              Enabled (2 type(s), 5 character(s) per type)
Total 1 local user(s) matched.
```

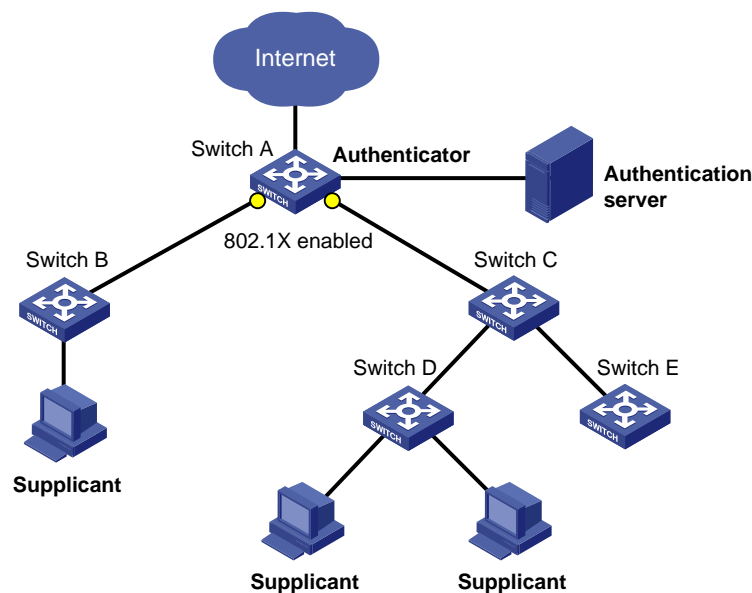
HABP configuration

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 49](#), 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 an 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 49 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 [Figure 49](#)), 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.

△ CAUTION:

- 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 the *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.

Follow these steps to configure an HABP server:

| To do... | Use the command... | Remarks |
|---|--|---|
| Enter system view | system-view | — |
| Enable HABP | habp enable | Optional Enabled by default |
| Configure HABP to work in server mode and specify the VLAN for HABP packets | habp server vlan <i>vlan-id</i> | Required HABP works in client mode by default. |
| Set the interval to send HABP requests | habp timer <i>interval</i> | Optional 20 seconds by default |

NOTE:

The VLAN specified on the HABP server for transmitting HABP packets must be the same as that to which the HABP clients belong.

Configuring an HABP client

An HABP client is usually configured on each device 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.

Follow these steps to configure an HABP client:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|--------------------------------|
| Enter system view | system-view | — |
| Enable HABP | habp enable | Optional Enabled by default |

| To do... | Use the command... | Remarks |
|---|--|---|
| Configure HABP to work in client mode | undo habp server | Optional HABP works in client mode by default. |
| Specify the VLAN to which the HABP client belongs | habp client vlan <i>vlan-id</i> | Optional By default, an HABP client belongs to VLAN 1. |

NOTE:

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

| To do... | Use the command... | Remarks |
|--|--|-----------------------|
| Display HABP configuration information | display habp [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display HABP MAC address table entries | display habp table [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display HABP packet statistics | display habp traffic [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

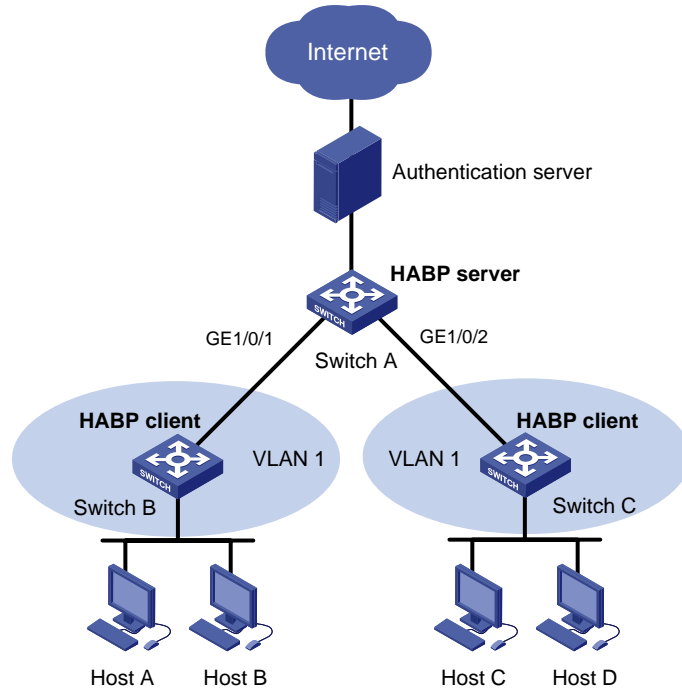
HABP configuration example

Network requirements

As shown in [Figure 50](#), access devices Switch B and Switch C are connected to Switch A. 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.
- On Switch A, configure the HABP server to send HABP request packets to the HABP clients in VLAN 1 at an interval of 50 seconds.

Figure 50 Network diagram for HABP configuration



Configuration procedure

1. Configure Switch A

Perform 802.1X related configurations on Switch A. For more information about 802.1X configurations, see the chapter “802.1X configuration.”

Enable HABP. (Because 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. (Because HABP is enabled by default, this configuration is optional.)

```
<SwitchA> system-view  
[SwitchB] habp enable
```

Configure HABP to work in client mode. (Because 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. (Because 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 |

Public key configuration

Asymmetric key algorithm overview

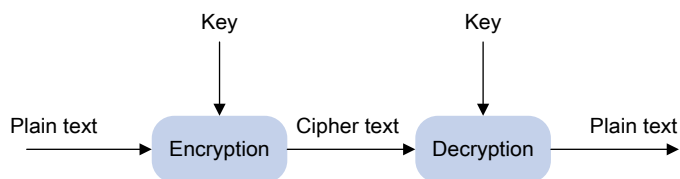
Basic concepts

- Algorithm: A set of transformation rules for encryption and decryption.
- Plain text: Information without being encrypted.
- Cipher text: Encrypted information.
- Key: A string of characters that controls the transformation between plain text and cipher text. It is used in both the encryption and decryption.

Key algorithm types

The information in plain text is encrypted by an algorithm with the help of a key before being sent. The resulting cipher text is transmitted across the network to the receiver, where it is decrypted by the same algorithm with the help of a key to obtain the original plain text.

Figure 51 Encryption and decryption



The following types of key algorithms are available, based on whether the keys for encryption and decryption are the same:

- Symmetric key algorithm—The keys for encryption and decryption are the same. Commonly used symmetric key algorithms include Advanced Encryption Standard (AES) and Data Encryption Standard (DES).
- 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 algorithm applications

Asymmetric key algorithms can be used for encryption and digital signature.

- Encryption—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 ensures confidentiality.

- 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.

The Revest-Shamir-Adleman Algorithm (RSA), and the Digital Signature Algorithm (DSA) are both asymmetric key algorithms. RSA can be used for data encryption/decryption and signature, whereas DSA is used for signature only.

NOTE:

Symmetric key algorithms are often used to encrypt/decrypt data for security. Asymmetric key algorithms are usually used in digital signature applications for peer identity authentication because they involve complex calculations and are time-consuming. In digital signature applications, only the digests, which are relatively short, are encrypted.

Configuring the local asymmetric key pair

You can create and destroy a local asymmetric key pair, and export the host public key of a local asymmetric key pair.

Creating an asymmetric key pair

Follow these steps to create an asymmetric key pair:

| To do... | Use the command... | Remarks |
|---|--|---|
| Enter system view | system-view | — |
| Create a local DSA key pair, or RSA key pairs | public-key local create { dsa rsa } | Required By default, no key pair is created. |

The **public-key local create rsa** command generates two key pairs: one server key pair and one host key pair. Each key pair comprises a public key and a private key. The **public-key local create dsa** command generates only one key pair, the host key pair.

After you enter the command, you are asked to specify the modulus length. The length of an RAS or DSA key modulus ranges from 512 to 2048 bits. To achieve higher security, specify a modulus at least 768 bits.

NOTE:

Key pairs created with the **public-key local create** command are saved automatically and can survive system reboots.

Displaying or exporting the local RSA or DSA host public key

You can display the local RSA or DSA host public key on the screen or export it to a specified file. Then, you can configure the local RSA or DSA host public key on the remote end so that the remote end can use the host public key to authenticate the local end through digital signature.

Follow these steps to display or export the local RSA or DSA host public key:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Display the local RSA host public key on the screen in a specified format, or export it to a specified file | public-key local export rsa { openssh ssh1 ssh2 } [<i>filename</i>] | Select a command according to the type of the key to be exported. |
| Display the local DSA host public key on the screen in a specified format or export it to a specified file | public-key local export dsa { openssh ssh2 } [<i>filename</i>] | |

Destroying an asymmetric key pair

You may need to destroy an 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 certificate from the Certificate Authority (CA) expires. To check the certificate status, use the **display pki certificate** command. For more information about the CA and certificate, see the chapter “PKI configuration.”

Follow these steps to destroy an asymmetric key pair:

| To do... | Use the command... | Remarks |
|--------------------------------|---|----------|
| Enter system view | system-view | — |
| Destroy an asymmetric key pair | public-key local destroy { dsa rsa } | Required |

Configuring a peer public key

To enable your local host to authenticate a peer, configure the peer RSA or DSA public key on the local host. The following methods are available:

- Import it from a public key file—Obtain a copy of the peer public key file through FTP or TFTP (in binary mode) first, and then import the public key from the file. During the import process, the system automatically converts the public key to a string in the Public Key Cryptography Standards (PKCS) format. HP recommends that you follow this method to configure the peer public key.
- Configure it manually—If the peer is an HP device, you can use the **display public-key local public** command to view and record its public key. On the local host, input or copy the key data in public key code view. A public key displayed by other methods may not in the PKCS format, and the system cannot save the format-incompliant key.

NOTE:

The device supports up to 20 peer public keys.

Follow these steps to import a peer host public key from the public key file:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|--|--|----------|
| Import the peer host public key from the public key file | public-key peer <i>keyname</i> import sshkey <i>filename</i> | Required |

Follow these steps to configure a peer public key manually:

| To do... | Use the command... | Remarks |
|--|---------------------------------------|--|
| Enter system view | system-view | — |
| Specify a name for a peer public key and enter public key view | public-key peer <i>keyname</i> | Required |
| Enter public key code view | public-key-code begin | — |
| Configure the peer host or server public key | Type or copy the key | Required Spaces and carriage returns are allowed between characters. |
| Return to public key view | public-key-code end | Required When you exit public key code view, the system automatically saves the public key. |
| Return to system view | peer-public-key end | — |

NOTE:

Do not configure an RSA server public key of the peer for identity authentication in SSH applications. Authentication in SSH applications uses the RSA host public key. For more information about SSH, see the chapter “SSH2.0 configuration.”

Displaying and maintaining public keys

| To do... | Use the command... | Remarks |
|--|--|-----------------------|
| Display the public keys of the local key pairs | display public-key local { <i>dsa</i> <i>rsa</i> } public [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display the peer public keys | display public-key peer [brief name <i>publickey-name</i>] [{ begin exclude include } <i>regular-expression</i>] | |

Public key configuration examples

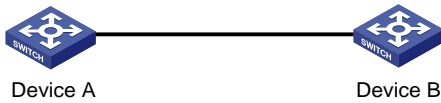
Configuring a peer public key manually

Network requirements

As shown in [Figure 52](#), to prevent illegal access, Device B authenticates Device A through a digital signature. Before configuring authentication parameters on Device B, configure the public key of Device A on Device B.

- Configure Device B to use the asymmetric key algorithm of RSA for identity authentication of Device A.
- Manually configure the host public key of Device A on Device B.

Figure 52 Network diagram for manually configuring a peer public key



Configuration procedure

1. Configure Device A.

Create RSA key pairs on Device A.

```
<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 created RSA key pairs.

```
[DeviceA] display public-key local rsa public
```

```
=====
Time of Key pair created: 09:50:06 2011/01/07
Key name: HOST_KEY
Key type: RSA Encryption Key
=====

Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F9854
C4421B57CAC64CFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A784A
D597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA80A
AB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001

=====

Time of Key pair created: 09:50:07 2011/01/07
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====

Key code:
307C300D06092A864886F70D0101010500036B003068026100999089E7AEE9802002D9EB2D0433B87BB6158E3
5000AFB3FF310E42F109829D65BF70F7712507BE1A3E0BC5C2C03FAAF00DFDDC63D004B4490DACBA3CFA9E84B
9151BDC7EECE1C8770D961557D192DE2B36CAF9974B7B293363BB372771C2C1F0203010001
```

2. Configure Device B.

Configure the host public key of Device A 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 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] public-key-code begin
code]30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814
F9854C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669
A784AD597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3B
CA80AAB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
[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:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F9854
C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A784A
D597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA80A
AB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

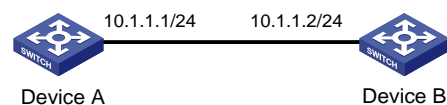
Importing a peer public key from a public key file

Network requirements

As shown in [Figure 53](#), to prevent illegal access, Device B authenticates Device A through a digital signature. Before configuring authentication parameters on Device B, configure the public key of Device A on Device B.

- Configure Device B to use the asymmetric key algorithm of RSA for identity authentication of Device A.
- Import the host public key of Device A from the public key file to Device B.

Figure 53 Network diagram for importing a peer public key from a public key file



Configuration procedure

1. Create key pairs on Device A and export the host public key.

Create RSA key pairs on Device A.

```
<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 created RSA key pairs.

```
[DeviceA] display public-key local rsa public
```

```
=====
Time of Key pair created: 09:50:06 2011/01/07
Key name: HOST_KEY
Key type: RSA Encryption Key
=====
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F9854
C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A784A
D597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA80A
AB5EE01986BD1EF64B42F17CCAE4A77F1EF999B2BF9C4A10203010001
```

```
=====
Time of Key pair created: 09:50:07 2011/01/07
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====
Key code:
307C300D06092A864886F70D0101010500036B003068026100999089E7AEE9802002D9EB2D0433B87BB6158E3
5000AFB3FF310E42F109829D65BF70F7712507BE1A3E0BC5C2C03FAAF00DFDDC63D004B4490DACBA3CFA9E84B
9151BDC7EECE1C8770D961557D192DE2B36CAF9974B7B293363BB372771C2C1F0203010001
```

Export the RSA host public key to a file named **devicea.pub**.

```
[DeviceA] public-key local export rsa ssh2 devicea.pub
[DeviceA] quit
```

2. Enable the FTP server function on Device B.

Enable the FTP server function, create an FTP user with the username **ftp**, password **123**, and user level **3**.

```
<DeviceB> system-view
[DeviceB] ftp server enable
[DeviceB] local-user ftp
[DeviceB-luser-ftp] password simple 123
[DeviceB-luser-ftp] service-type ftp
```

```
[DeviceB-luser-ftp] authorization-attribute level 3
[DeviceB-luser-ftp] quit
```

3. Upload the public key file of Device A to Device B.

FTP the public key file **devicea.pub** to Device B with the file transfer mode of binary.

```
<DeviceA> ftp 10.1.1.2
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2.
220 FTP service ready.
User(10.1.1.2:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.
[ftp] binary
200 Type set to I.
[ftp] put devicea.pub
227 Entering Passive Mode (10,1,1,2,5,148).
125 BINARY mode data connection already open, transfer starting for /devicea.pub.
226 Transfer complete.
FTP: 299 byte(s) sent in 0.189 second(s), 1.00Kbyte(s)/sec.
```

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] public-key peer devicea import sshkey devicea.pub
```

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:

```
30819F300D06092A864886F70D010101050003818D0030818902818100D90003FA95F5A44A2A2CD3F814F9854
C4421B57CAC64CFFE4782A87B0360B600497D87162D1F398E6E5E51E5E353B3A9AB16C9E766BD995C669A784A
D597D0FB3AA9F7202C507072B19C3C50A0D7AD3994E14ABC62DB125035EA326470034DC078B2BAA3BC3BCA80A
AB5EE01986BD1EF64B42F17CCA4E477F1EF999B2BF9C4A10203010001
```

PKI configuration

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

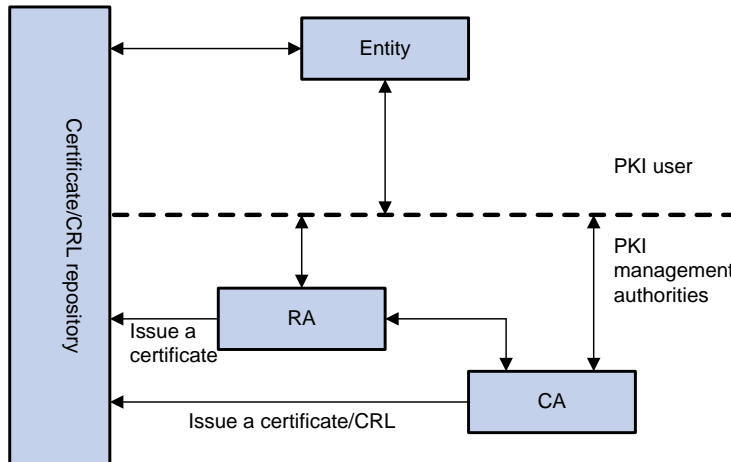
A CA policy is a set of criteria that a CA follows in processing certificate requests, issuing and revoking certificates, and publishing CRLs. Usually, a CA advertises its policy in the form of certification practice

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 check 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 54 PKI architecture



- Entity

An entity is an end user of PKI products or services, such as a person, an organization, a device like a router or a switch, 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 while providing 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 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 example, 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.

How does PKI work

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 works:

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 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, and the CA approves the request, updates the CRLs and publishes the CRLs on the LDAP server.

PKI configuration task list

Complete the following tasks to configure PKI:

| Task | Remarks | |
|--|---|---------------------|
| Configuring an entity DN | Required | |
| Configuring a PKI domain | Required | |
| Submitting a PKI certificate request | Submitting a certificate request in auto mode | Required |
| | Submitting a certificate request in manual mode | Use either approach |
| Retrieving a certificate manually | Optional | |
| Configuring PKI certificate verification | Optional | |
| Destroying a local RSA key pair | Optional | |
| Deleting a certificate | Optional | |

| Task | Remarks |
|--------------------------------------|----------|
| 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.

NOTE:

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.

Follow these steps to configure an entity DN:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Create an entity and enter its view | pki entity <i>entity-name</i> | Required No entity exists by default. |
| Configure the common name for the entity | common-name <i>name</i> | Optional No common name is specified by default. |
| Configure the country code for the entity | country <i>country-code-str</i> | Optional No country code is specified by default. |
| Configure the FQDN for the entity | fqdn <i>name-str</i> | Optional No FQDN is specified by default. |
| Configure the IP address for the entity | ip <i>ip-address</i> | Optional No IP address is specified by default. |

| To do... | Use the command... | Remarks |
|--|---|---|
| Configure the locality for the entity | locality <i>locality-name</i> | Optional No locality is specified by default. |
| Configure the organization name for the entity | organization <i>org-name</i> | Optional No organization is specified by default. |
| Configure the unit name for the entity | organization-unit <i>org-unit-name</i> | Optional No unit is specified by default. |
| Configure the state or province for the entity | state <i>state-name</i> | Optional No state or province is specified by default. |

NOTE:

- Up to two entities can be created on a device.
- 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 IKE and SSL, and only has local significance. A PKI domain configured on a device is invisible to the CA and other devices.

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, checks its qualification, and determines whether to ask the CA to sign a digital certificate. The RA only checks 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—Upon receiving the root certificate of the CA, an entity needs to verify the fingerprint of the root certificate—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.

Follow these steps to configure a PKI domain:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Create a PKI domain and enter its view | pki domain <i>domain-name</i> | Required No PKI domain exists by default. |
| Specify the trusted CA | ca identifier <i>name</i> | Required No trusted CA is specified by default. |
| Specify the entity for certificate request | certificate request entity <i>entity-name</i> | Required No entity is specified by default. The specified entity must exist. |
| Specify the authority for certificate request | certificate request from { ca ra } | Required No authority is specified by default. |
| Configure the URL for certificate request | certificate request url <i>url-string</i> | Required No certificate request URL is configured by default. |
| Configure the polling interval and attempt limit for querying the certificate request status | certificate request polling { count <i>count</i> interval <i>minutes</i> } | Optional The polling is executed for up to 50 times at the interval of 20 minutes by default. |
| Specify the LDAP server | ldap-server ip <i>ip-address</i> [port <i>port-number</i>] [version <i>version-number</i>] | Optional No LDP server is specified by default. |
| Configure the fingerprint for root certificate verification | root-certificate fingerprint { md5 sha1 } <i>string</i> | 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. |

NOTE:

- Up to two PKI domains can be created on a device.
- 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.

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 an online mode or an offline 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

In auto mode, an entity automatically requests a certificate from the CA server 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.

Follow these steps to configure an entity to submit a certificate request in auto mode:

| To do... | Use the command... | Remarks |
|--|--|-------------------------------|
| Enter system view | system-view | — |
| Enter PKI domain view | pki domain <i>domain-name</i> | — |
| Set the certificate request mode to auto | certificate request mode auto [key-length <i>key-length</i> password { cipher simple } <i>password</i>] * | Required Manual by default |

! 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.

Submitting a certificate request in manual mode

In manual mode, you manually submit a certificate request for an entity. Before submitting a certificate request, you must ensure that an RSA key pair has been generated and the CA certificate has been retrieved and saved locally.

The CA certificate is required to verify the authenticity and validity of a local certificate. The public key of the key pair is an important part of the request information and will be transferred to the CA along with some other information. For more information about RSA key pair configuration, see the *Security Configuration Guide*.

Follow these steps to submit a certificate request in manual mode:

| To do... | Use the command... | Remarks |
|--|---|-------------------------------|
| Enter system view | system-view | — |
| Enter PKI domain view | pki domain <i>domain-name</i> | — |
| Set the certificate request mode to manual | certificate request mode manual | Optional Manual by default |
| Return to system view | quit | — |
| Retrieve a CA certificate manually | See “ Retrieving a certificate manually ” | “Required” |

| To do... | Use the command... | Remarks |
|---|---|--|
| Generate a local RSA key pair | public-key local create rsa | Required No local RSA key pair exists by default. |
| Submit a local certificate request manually | pki request-certificate domain <i>domain-name</i> [<i>password</i>] [pkcs10 [filename <i>filename</i>]] | Required |

NOTE:

- If a PKI domain already has a local certificate, creating an RSA key pair will result in inconsistency between the key pair and the certificate. To generate a new RSA key pair, delete the local certificate and then issue the **public-key local create** command. For more information about the **public-key local create** command, see the *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, save the request information by using the **pki request-certificate domain** command with the **pkcs10** and **filename** keywords, and then send the file to the CA by an out-of-band means.
- Make sure the clocks of the entity and the CA are synchronous. Otherwise, the validity period of the certificate will be abnormal.
- The **pki request-certificate domain** configuration will not be saved in the configuration file.

Retrieving a certificate manually

You can download CA certificates and local certificates and save them locally. To do so, use either the online mode or the offline 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 two purposes:

- Locally store the certificates associated with the local security domain for improved query efficiency and reduced query count
- Prepare for certificate verification.

Before retrieving a local certificate in online mode, be sure to complete the LDAP server configuration.

Follow these steps to retrieve a certificate manually:

| To do... | Use the command... | Remarks |
|---------------------------------|--|---------------------|
| Enter system view | system-view | — |
| Retrieve a certificate manually | Online pki retrieval-certificate { ca local } domain <i>domain-name</i> | Required |
| | Offline pki import-certificate { ca local } domain <i>domain-name</i> { der p12 pem } [filename <i>filename</i>] | Use either command. |

△ CAUTION:

- 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 **pki retrieval-certificate** configuration will not be saved in the configuration file.
- Be sure that the device system time falls in the validity period of the certificate so that the certificate is valid.

Configuring PKI certificate verification

A certificate needs to be verified before being used. Verifying a certificate is to check whether the certificate is signed by the CA and whether the certificate has expired or been revoked.

Before verifying a certificate, you must retrieve the CA certificate.

You can specify whether CRL checking is required in certificate verification. If you enable CRL checking, CRLs will be used in verification of a certificate.

Configuring CRL-checking-enabled PKI certificate verification

Follow these steps to configure CRL-checking-enabled PKI certificate verification:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Enter PKI domain view | pki domain <i>domain-name</i> | — |
| Specify the URL of the CRL distribution point | crl url <i>url-string</i> | Optional No CRL distribution point URL is specified by default. |
| Set the CRL update period | crl update-period <i>hours</i> | Optional By default, the CRL update period depends on the next update field in the CRL file. |
| Enable CRL checking | crl check enable | Optional Enabled by default |
| Return to system view | quit | — |
| Retrieve the CA certificate | See “ Retrieving a certificate manually ” | Required |
| Retrieve CRLs | pki retrieval-crl domain <i>domain-name</i> | Required |
| Verify the validity of a certificate | pki validate-certificate { ca local } domain <i>domain-name</i> | Required |

Configuring CRL-checking-disabled PKI certificate verification

Follow these steps to configure CRL-checking-disabled PKI certificate verification:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|--|---|--------------------------------|
| Enter PKI domain view | pki domain <i>domain-name</i> | — |
| Disable CRL checking | crl check disable | Required Enabled by default |
| Return to system view | quit | — |
| Retrieve the CA certificate | See “ Retrieving a certificate manually ” | Required |
| Verify the validity of the certificate | pki validate-certificate { ca local } domain <i>domain-name</i> | Required |

NOTE:

- The CRL update period refers to the interval at which the entity downloads CRLs from the CRL server. The CRL update period configured manually is prior to that specified in the CRLs.
- The **pki retrieval-crl domain** configuration will not be saved in the configuration file.
- The URL of the CRL distribution point does not support domain name resolution.

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, destroy the old RSA key pair and then create a pair to request a new certificate.

Follow these steps to destroy a local RSA key pair:

| To do... | Use the command... | Remarks |
|------------------------------|-------------------------------------|----------|
| Enter system view | system-view | — |
| Destroy a local RSA key pair | public-key local destroy rsa | Required |

NOTE:

For more information about the **public-key local destroy** command, see the *Security Command Reference*.

Deleting a certificate

When a certificate requested manually is about to expire or you want to request a new certificate, delete the current local certificate or CA certificate.

Follow these steps to delete a certificate:

| To do... | Use the command... | Remarks |
|---------------------|---|----------|
| Enter system view | system-view | — |
| Delete certificates | pki delete-certificate { ca local } domain <i>domain-name</i> | Required |

Configuring an access control policy

A certificate attribute-based access control policy can further control access to the server, providing additional security for the server.

Follow these steps to configure a certificate attribute-based access control policy:

| To do... | Use the command... | Remarks |
|--|--|---|
| Enter system view | system-view | — |
| Create a certificate attribute group and enter its view | pki certificate attribute-group <i>group-name</i> | Required No certificate attribute group exists by default. |
| Configure an attribute rule for the certificate issuer name, certificate subject name, or alternative subject name | attribute <i>id</i> { alt-subject-name { fqdn ip } { issuer-name subject-name } { dn fqdn ip } } { ctn equ nctn nequ } <i>attribute-value</i> | Optional No restriction is defined on the issuer name, certificate subject name and alternative subject name by default. |
| Return to system view | quit | — |
| Create a certificate attribute-based access control policy and enter its view | pki certificate access-control-policy <i>policy-name</i> | Required No access control policy exists by default. |
| Configure a certificate attribute-based access control rule | rule [<i>id</i>] { deny permit } <i>group-name</i> | Required No access control rule exists by default. |

CAUTION:

A certificate attribute group must exist to be associated with a rule.

Displaying and maintaining PKI

| To do... | Use the command... | Remarks |
|--|---|-----------------------|
| Display the contents or request status of a certificate | display pki certificate { { ca local } domain <i>domain-name</i> request-status } [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |
| Display CRLs | display pki crl domain <i>domain-name</i> [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |
| Display information about one or all certificate attribute groups | display pki certificate attribute-group { <i>group-name</i> all } [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |
| Display information about one or all certificate attribute-based access control policies | display pki certificate access-control-policy { <i>policy-name</i> all } [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |

PKI configuration examples

⚠ CAUTION:

- 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.

Requesting a certificate from a CA running RSA Keon

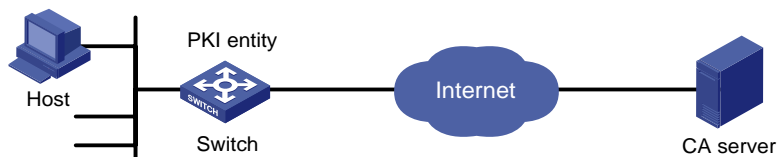
NOTE:

The CA server runs RSA Keon in this configuration example.

Network requirements

- The device submits a local certificate request to the CA server.
- The device acquires the CRLs for certificate verification.

Figure 55 Request a certificate from a CA running RSA Keon



Configuration procedure

1. Configure the CA server

Create a CA server named **myca**.

In this example, 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).

The other attributes might be left using the default values.

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.

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 HTTP and set the HTTP URL to `http://4.4.4.133:447/myca.crl`.

After the configuration, make sure that the system clock of the device is synchronous to that of the CA, so that the device can request certificates and retrieve CRLs properly.

2. Configure the switch

- Configure the entity DN

Configure the entity name as **aaa** and the common name as **switch**.

```
<Switch> system-view
[Switch] pki entity aaa
[Switch-pki-entity-aaa] common-name switch
[Switch-pki-entity-aaa] quit
```

- Configure the PKI domain

Create PKI domain **torsa** and enter its view.

```
[Switch] pki domain torsa
```

Configure the name of the trusted CA as **myca**.

```
[Switch-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.

```
[Switch-pki-domain-torsa] certificate request url
http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

Set the registration authority to **CA**.

```
[Switch-pki-domain-torsa] certificate request from ca
```

Specify the entity for certificate request as **aaa**.

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

Configure the URL for the CRL distribution point.

```
[Switch-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl
[Switch-pki-domain-torsa] quit
```

- Generate a local key pair using RSA

```
[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 in the modulus [default = 1024]:

Generating Keys...

```
+++++
+++++
+++++
+++++
```

- Apply for certificates

Retrieve the CA certificate and save it locally.

```
[Switch] 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.

[Switch] pki retrieval-crl domain torsa
Connecting to server for retrieving CRL. Please wait a while.....
CRL retrieval success!

Request a local certificate manually.

[Switch] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait.....
[Switch]
Enrolling the local certificate,please wait a while.....
Certificate request Successfully!
Saving the local certificate to device.....
Done!

3. Verify your configuration

Use the following command to view information about the local certificate acquired.

[Switch] 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 2011 GMT
    Not After : Jan  8 09:26:53 2011 GMT
  Subject:
    CN=switch
  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 C9CDD38 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 some other **display** commands—**display pki certificate ca domain** and **display pki crl domain** commands—to view detailed information about the CA certificate and CRLs. For more information about the commands, see the *Security Command Reference*.

Requesting a certificate from a CA running Windows 2003 Server

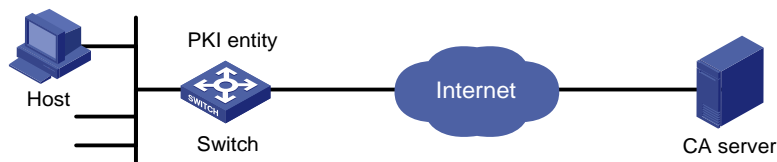
NOTE:

The CA server runs the Windows 2003 server in this configuration example.

Network requirements

Configure PKI entity Switch to request a local certificate from the CA server.

Figure 56 Request a certificate from a CA running Windows 2003 server



Configuration procedure

1. Configure the CA server
 - Install the certificate service suites

From the start menu, select **Control Panel > Add or Remove Programs**, and then select **Add/Remove Windows Components > Certificate Services** and click **Next** to begin the installation.

- 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.

- Modify the certificate service attributes

From the start menu, select **Control Panel > Administrative Tools > Certificate Authority**. If the CA server and SCEP add-on have been installed successfully, there should be two certificates issued by the CA to the RA. Right-click on the CA server in the navigation tree and select **Properties > Policy Module**. Click **Properties** and then select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.**

- Modify the Internet Information Services (IIS) attributes

From the start menu, select **Control Panel > Administrative Tools > Internet Information Services (IIS) Manager** and then select **Web Sites** from the navigation tree. Right-click on **Default Web Site** and select **Properties > Home Directory**. Specify the path for certificate service in the **Local path** text box. In addition, specify an available port number as the TCP port number of the default website to avoid conflict with existing services.

After completing the configuration, check that the system clock of the switch is synchronous to that of the CA server, ensuring that the switch can request a certificate normally.

2. Configure the switch

- Configure the entity DN

Configure the entity name as **aaa** and the common name as **switch**.

```
<Switch> system-view
[Switch] pki entity aaa
[Switch-pki-entity-aaa] common-name switch
[Switch-pki-entity-aaa] quit
```

- Configure the PKI domain

Create PKI domain **torsa** and enter its view.

```
[Switch] pki domain torsa
```

Configure the name of the trusted CA as **myca**.

```
[Switch-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.

```
[Switch-pki-domain-torsa] certificate request url
http://4.4.4.1:8080/certsrv/mscep/mscep.dll
```

Set the registration authority to **RA**.

```
[Switch-pki-domain-torsa] certificate request from ra
```

Specify the entity for certificate request as **aaa**.

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

- Generate a local key pair using RSA

```
[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 in the modulus [default = 1024]:

Generating Keys...

```
+++++
+++++
```

```
+++++
+++++
```

- **Apply for certificates**

Retrieve the CA certificate and save it locally.

```
[Switch] 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.

```
[Switch] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait.....
[Switch]
Enrolling the local certificate,please wait a while.....
Certificate request Successfully!
Saving the local certificate to device.....
Done!
```

3. Verify your configuration

Use the following command to view information about the local certificate acquired.

```
[Switch] 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 2011 GMT
      Not After : Feb 21 12:42:16 2011 GMT
    Subject:
      CN=switch
    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 7ABCE3EA 9BF385F8 A448F4E1
X509v3 Authority Key Identifier:
keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

X509v3 CRL Distribution Points:
URI:http://100192b/CertEnroll/CA%20server.crl
URI:file://\\100192b\CertEnroll\CA server.crl

Authority Information Access:
CA Issuers - URI:http://100192b/CertEnroll/100192b_CA%20server.crt
CA Issuers - URI:file://\\100192b\CertEnroll\100192b_CA server.crt

1.3.6.1.4.1.311.20.2:
.O.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)

```

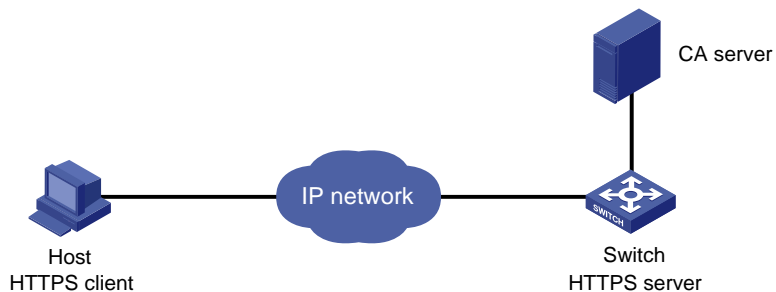
You can also use some other **display** commands—such as, **display pki certificate ca domain** command—to view more information about the CA certificate. For more information about the command, see the *Security Command Reference*.

Configuring a certificate attribute-based access control policy

Network requirements

- The client accesses the remote HTTP Secure (HTTPS) server through the HTTPS protocol.
- Configure SSL to ensure that only legal clients log in to the HTTPS server.
- Create a certificate attribute-based access control policy to control access to the HTTPS server.

Figure 57 Configure a certificate attribute-based access control policy



Configuration procedure

NOTE:

- For more information about SSL configuration, see the chapter “SSL configuration.”
 - For more information about HTTPS configuration, see the *Fundamentals Configuration Guide*.
 - The PKI domain to be referenced by the SSL policy must be created in advance. For how to configure a PKI domain, see “[Configure the PKI domain.](#)”
-

1. Configure the HTTPS server

Configure the SSL policy for the HTTPS server to use.

```
<Switch> system-view
[Switch] ssl server-policy myssl
[Switch-ssl-server-policy-myssl] pki-domain 1
[Switch-ssl-server-policy-myssl] client-verify enable
[Switch-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.

```
[Switch] pki certificate attribute-group mygroup1
[Switch-pki-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn aabbcc
[Switch-pki-cert-attribute-group-mygroup1] attribute 2 issuer-name ip equ 10.0.0.1
[Switch-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**.

```
[Switch] pki certificate attribute-group mygroup2
[Switch-pki-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn apple
[Switch-pki-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn aabbcc
[Switch-pki-cert-attribute-group-mygroup2] quit
```

3. Configure the certificate attribute-based access control policy

Create the certificate attribute-based access control policy of **myacp** and add two access control rules.

```
[Switch] pki certificate access-control-policy myacp
[Switch-pki-cert-acp-myacp] rule 1 deny mygroup1
[Switch-pki-cert-acp-myacp] rule 2 permit mygroup2
[Switch-pki-cert-acp-myacp] quit
```

4. Apply the SSL server policy and certificate attribute-based access control policy to HTTPS service and enable HTTPS service.

Apply SSL server policy **myssl** to HTTPS service.

```
[Switch] ip https ssl-server-policy myssl
```

Apply the certificate attribute-based access control policy of **myacp** to HTTPS service.

```
[Switch] ip https certificate access-control-policy myacp
```

Enable HTTPS service.

```
[Switch] ip https enable
```

Troubleshooting PKI

Failed to retrieve a CA certificate

Symptom

Failed to retrieve a CA certificate.

Analysis

Possible reasons include:

- 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 device is not synchronized with that of the CA.

Solution

- Make sure that the network connection is physically proper.
- Check that the required commands are configured properly.
- Use the **ping** command to check that the RA server is reachable.
- Specify the authority for certificate request.
- Synchronize the system clock of the device with that of the CA.

Failed to request a local certificate

Symptom

Failed to request a local certificate.

Analysis

Possible reasons include:

- 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 that the network connection is physically proper.
- Retrieve a CA certificate.
- Regenerate a key pair.
- Specify a trusted CA.

- Use the **ping** command to check 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

Possible reasons include:

- 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.

Solution

- Make sure that 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.

SSH2.0 configuration

SSH2.0 overview

Introduction to SSH2.0

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 device 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.

NOTE:

- When acting as an SSH server, the device supports SSH2.0 and SSH1. When acting as an SSH client, the device supports SSH2.0 only.
 - Unless otherwise noted, SSH in this document refers to SSH2.0.
-

How does SSH work

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 11](#).

Table 11 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. |
| 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 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. Upon 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 are transferred in plain text.

Key and algorithm negotiation

1. The server and the client send algorithm negotiation packets to each other, which include the supported public key algorithms list, encryption algorithms list, Message Authentication Code (MAC) algorithms list, and compression algorithms list.
2. 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.
3. 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.

△ CAUTION:

Before the negotiation, the server must have already generated a DSA or RSA key pair, which is used in generating the session key and by the client to authenticate the identity of the server. For more information about DSA and RSA key pairs, see the chapter "Public key configuration."

Authentication

SSH provides password authentication and publickey authentication.

- Password authentication—The server uses AAA for authentication of the client. During password authentication, the client encrypts its username and password, encapsulates them into a password authentication request, and sends the request to the server. Upon receiving the request, the 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.
- 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 device supports using the publickey algorithms RSA and DSA for digital signature.

The following gives the steps of the authentication stage:

1. The client sends the server an authentication request that includes the username, authentication method (password authentication or publickey authentication), and 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 process repeats until the authentication succeeds, or the number of failed authentication attempts exceeds the maximum of authentication attempts and the session is torn down.

NOTE:

In addition to password authentication and publickey authentication, SSH2.0 also provides the following authentication methods:

- **password-publickey**—Performs both password authentication and publickey authentication if the client is using SSH2.0 and performs either if the client is running SSH1.
 - **any**—Performs either password authentication or publickey authentication.
-

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. After successfully processing the request, the server sends an SSH_MSG_SUCCESS packet to the client and goes on to the interaction stage with the client. Otherwise, the server sends an SSH_MSG_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 in the following way:

- The client encrypts and sends the command to be executed to the server.
- The server decrypts and executes the command, and then encrypts and sends the result to the client.
- The client decrypts and displays the result on the terminal.

NOTE:

- In the interaction stage, you can execute commands from the client by pasting the commands in text format—the text must be within 2000 bytes. The commands should be in the same view. Otherwise, the server might not be able to perform the commands correctly.
 - If the command text exceeds 2000 bytes, you can execute the commands by saving the text as a configuration file, uploading the configuration file to the server through Secure FTP (SFTP), and then using the configuration file to restart the server.
-

Configuring the device as an SSH server

SSH server configuration task list

Complete the following tasks to configure an SSH server:

| Task | Remarks |
|---|--|
| Generating a DSA or RSA key pair | Required |
| 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 |

Generating a DSA or RSA key pair

In the key and algorithm negotiation stage, the DSA or RSA key pair is required to generate the session ID and for the client to authenticate the server.

Follow these steps to generate a DSA or RSA key pair on the SSH server:

| To do... | Use the command... | Remarks |
|--------------------------------|--|---|
| Enter system view | system-view | — |
| Generate a DSA or RSA key pair | public-key local create { dsa rsa } | Required By default, neither DSA key pair nor RSA key pair exists. |

NOTE:

- For more information about the **public-key local create** command, see the *Security Command Reference*.
- To support SSH clients using different types of key pairs, generate both DSA and RSA key pairs on the SSH server.
- The **public-key local create rsa** command generates a server key pair and a host 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 respectively, no session key transmission is required in SSH2.0 and the server key pair is not used.
- The length of the modulus of RSA server keys and host keys must be in the range 512 to 2048 bits. Some SSH2.0 clients require that the length of the key modulus be at least 768 bits on the SSH server side.
- The **public-key local create dsa** command generates only the host key pair. SSH1 does not support the DSA algorithm.
- The length of the modulus of DSA host keys must be in the range 512 to 2048 bits. Some SSH2.0 clients require that the length of the key modulus be at least 768 bits on the SSH server side.

Enabling the SSH server function

Follow these steps to enable the SSH server function:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|--------------------------------|--------------------------|---------------------------------|
| Enable the SSH server function | ssh server enable | Required Disabled by default |

Configuring the user interfaces for SSH clients

An SSH client accesses the device 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 logging in after the configuration.

Follow these steps to configure the protocols for the current user interface to support:

| To do... | Use the command... | Remarks |
|--|--|--|
| Enter system view | system-view | — |
| Enter user interface view of one or more user interfaces | user-interface vty <i>number</i> [<i>ending-number</i>] | — |
| Set the login authentication mode to scheme | authentication-mode scheme | Required By default, the authentication mode is password . |
| Configure the user interface(s) to support SSH login | protocol inbound { all ssh } | Optional All protocols are supported by default. |

CAUTION:

- For more information about the **authentication-mode** and **protocol inbound** commands, see the *Fundamentals Command Reference*.
- 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.

Configuring a client public key

NOTE:

This configuration task is only necessary for SSH users using publickey authentication.

For each SSH user that uses publickey authentication to login, 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.

To configure the public key of an SSH client, you can configure it manually or import it from the public key file:

- Configure it manually—You can input or copy the public key to the SSH server. The public key must be in the distinguished encoding rules (DER) encoding format and have not been converted.
- Import it from the public key file—During the import process, the system will automatically convert the public key to a string coded using the Public Key Cryptography Standards (PKCS). Before

importing the public key, you must upload the public key file (in binary) to the local host through FTP or TFTP.

△ CAUTION:

- HP recommends you to configure a client public key by importing it from a public key file.
- You can configure up to 20 client public keys on an SSH server.

Configuring a client public key manually

Follow these steps to configure the client public key manually:

| To do... | Use the command... | Remarks |
|---|---------------------------------------|---|
| Enter system view | system-view | — |
| Enter public key view | public-key peer <i>keyname</i> | — |
| Enter public key code view | public-key-code begin | — |
| Configure a client public key | Enter the content of the public key | Required Spaces and carriage returns are allowed between characters. |
| Return from public key code view to public key view | public-key-code end | — When you exit public key code view, the system automatically saves the public key. |
| Return from public key view to system view | peer-public-key end | — |

Importing a client public key from a public key file

Follow these steps to import a public key from a public key file:

| To do... | Use the command... | Remarks |
|--|--|----------|
| Enter system view | system-view | — |
| Import the public key from a public key file | public-key peer <i>keyname</i> import sshkey <i>filename</i> | Required |

NOTE:

For more information about client side public key configuration and the relevant commands, see the *Security Configuration Guide*.

Configuring an SSH user

This configuration allows you to create an SSH user and specify the service type and authentication method. An SSH user's service type can be Secure Telnet (Stelnet) or Secure FTP (SFTP). For more information about Stelnet, see "[SSH2.0 overview](#)." For more information about SFTP, see the chapter "SFTP configuration."

To use publickey authentication, you must configure the user account and the user's public key on the SSH server. To use password authentication, you can configure the user account on either the device or the remote authentication server, such as a RADIUS authentication server.

Follow these steps to configure an SSH user and specify the service type and authentication mode:

| To do... | | Use the command... | Remarks |
|--|-----------------------------|--|---------------------|
| Enter system view | | system-view | — |
| Create an SSH user, and specify the service type and authentication mode | For Stelnet users | ssh user <i>username</i> service-type stelnet authentication-type { password { any password-publickey publickey } assign publickey <i>keyname</i> } | Required |
| | For all users or SFTP users | ssh user <i>username</i> service-type { all sftp } authentication-type { password { any password-publickey publickey } assign publickey <i>keyname</i> work-directory <i>directory-name</i> } | Use either command. |

⚠ CAUTION:

- A user without an SSH account can still pass password authentication and log in to the server through Stelnet or SFTP, as long as the user can pass AAA authentication and the service type is SSH.
- An SSH server supports up to 1024 SSH users.
- For successful login through SFTP, you must set the user service type to **sftp** or **all**.
- SSH1 does not support the service type **sftp**. If the client uses SSH1 to log in to the server, you must set the service type to **stelnet** or **all** on the server.
- An SFTP user's working folder depends on the authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both the publickey and password authentication methods, the working folder is the one set by using the **ssh user** command.
- You can change the authentication method and public key of an SSH user when the user is communicating with the SSH server, but your changes take effect only after the user logs out and logs in again.

NOTE:

- With publickey authentication, which commands a user can use after login depends on the user privilege level, which is configured with the **user privilege level** command on the user interface.
- With password authentication, which commands a user can use after login depends on AAA authorization.

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 the parameters can help avoid malicious guessing at and cracking of the keys and usernames, securing your SSH connections.

Follow these steps to set the SSH management parameters:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Enable the SSH server to support SSH1 clients | ssh server compatible-ssh 1x enable | Optional By default, the SSH server supports SSH1 clients. |
| Set the RSA server key pair update interval | ssh server rekey-interval <i>hours</i> | Optional By default, the interval is 0, and the RSA server key pair is not updated. |
| Set the SSH user authentication timeout period | ssh server authentication-timeout <i>time-out-value</i> | Optional 60 seconds by default |
| Set the maximum number of SSH authentication attempts | ssh server authentication-retries <i>times</i> | Optional 3 by default |

NOTE:

Authentication will fail if the number of authentication attempts—including both publickey and password authentication—exceeds that specified in the **ssh server authentication-retries** command.

Configuring the device as an SSH client

SSH client configuration task list

Complete the following tasks to configure an SSH client:

| 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 |

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 do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| 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 } | Required Select either approach By default, an SSH |

| To do... | Use the command... | Remarks |
|---|---|--|
| Specify a source IPv6 address or interface for the SSH client | ssh client ipv6 source { ipv6 ipv6-address interface interface-type interface-number } | client uses the IP address of the interface specified by the route of the device to access the SSH server. |

Configuring whether first-time authentication is supported

When the device connects to the SSH server as an SSH client, you can configure whether the device 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.

Enable the device to support first-time authentication

Follow these steps to enable the device to support first-time authentication:

| To do... | Use the command... | Remarks |
|--|-------------------------------------|---|
| Enter system view | system-view | — |
| Enable the device to support first-time authentication | ssh client first-time enable | Optional By default, first-time authentication is supported on a client. |

Disable 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.

Follow these steps to disable first-time authentication:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Disable first-time authentication support | undo ssh client first-time | Required By default, first-time authentication is supported on a client. |
| Configure the server host public key | See “Configuring a client public key.” | Required The method for configuring the server host public key on the client is similar to that for configuring client public key on the server. |
| Specify the host public key name of the server | ssh client authentication server <i>server assign publickey keyname</i> | Required |

Establishing a connection between the SSH client and server

Follow these steps to establish the connection between the SSH client and the server:

| To do... | | Use the 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 | ssh2 server [<i>port-number</i>] [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 }] * | Required |
| | For an IPv6 server | ssh2 ipv6 server [<i>port-number</i>] [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 }] * | Use either command in user view. |

Displaying and maintaining SSH

| To do... | Use the command... | Remarks |
|--|--|-----------------------|
| Display the source IP address or interface currently set for the SFTP client | display sftp client source [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display the source IP address or interface currently set for the SSH client | display ssh client source [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display SSH server status information or session information on an SSH server | display ssh server { status session } [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display the mappings between SSH servers and their host public keys saved on an SSH client | display ssh server-info [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display information about a specified or all SSH users on the SSH server | display ssh user-information [<i>username</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display the public keys of the local key pairs | display public-key local { dsa rsa } public [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display the public keys of the SSH peers | display public-key peer [brief name <i>publickey-name</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

NOTE:

For more information about the **display public-key local** and **display public-key peer** commands, see the *Security Command Reference*.

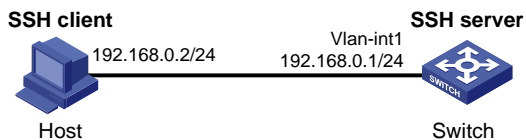
SSH server configuration examples

When switch acts as server for password authentication

Network requirements

As shown in [Figure 58](#), an SSH connection is required between the host and the switch for secure data exchange. Use password authentication and configure a username and password for the host on the switch.

Figure 58 Switch acts as server for password authentication



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 4
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

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

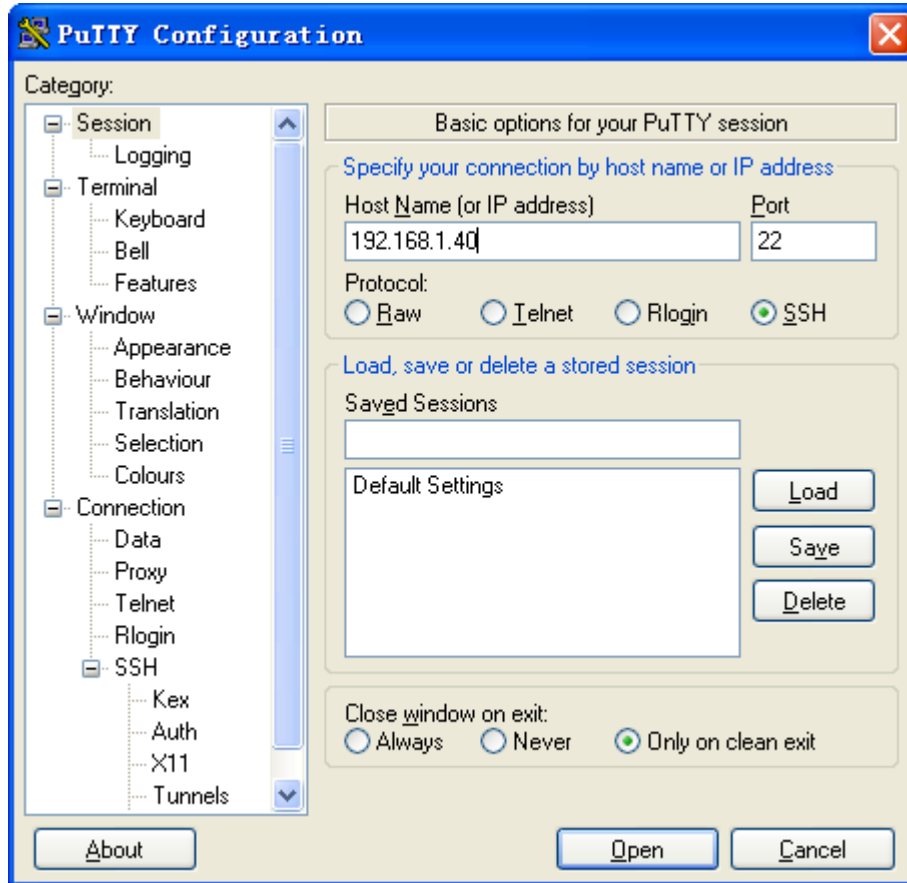
NOTE:

The device supports many types of SSH client software, such as PuTTY, and OpenSSH. The following is an example of configuring SSH client using PuTTY Version 0.58.

Establish a connection to the SSH server.

Launch PuTTY.exe to enter the following interface. In the **Host Name or IP address** text box, enter the IP address of the server—192.168.1.40.

Figure 59 SSH client configuration interface



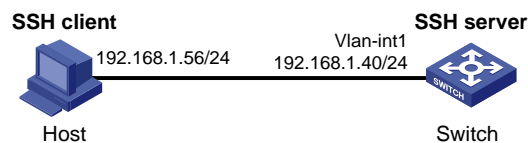
Click **Open** to connect to the server. If the connection is normal, you will be prompted to enter the username and password. After entering the username **client001** and password **aabbcc**, you can enter the configuration interface of the server.

When switch acts as server for publickey authentication

Network requirements

As shown in Figure 60, an SSH connection is required between the host and the switch for secure data exchange. Use publickey authentication and the RSA public key algorithm.

Figure 60 Switch acts as server for publickey authentication



Configuration procedure

NOTE:

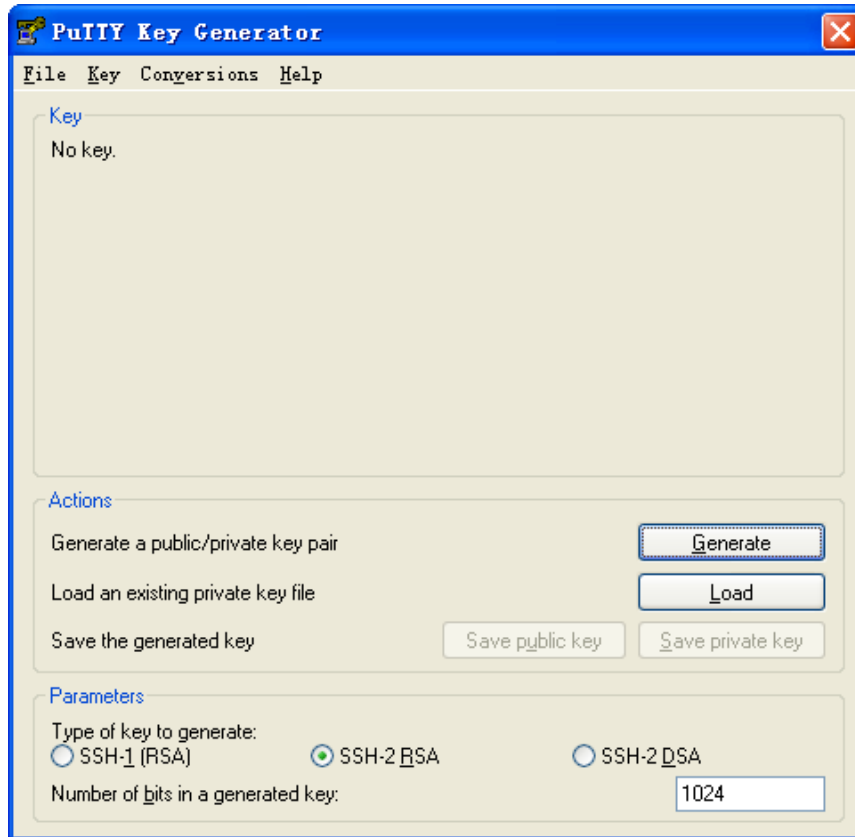
During SSH server configuration, the client public key is required. Use the client software to generate RSA key pairs on the client before configuring the SSH server.

1. Configure the SSH client

Generate the RSA key pairs.

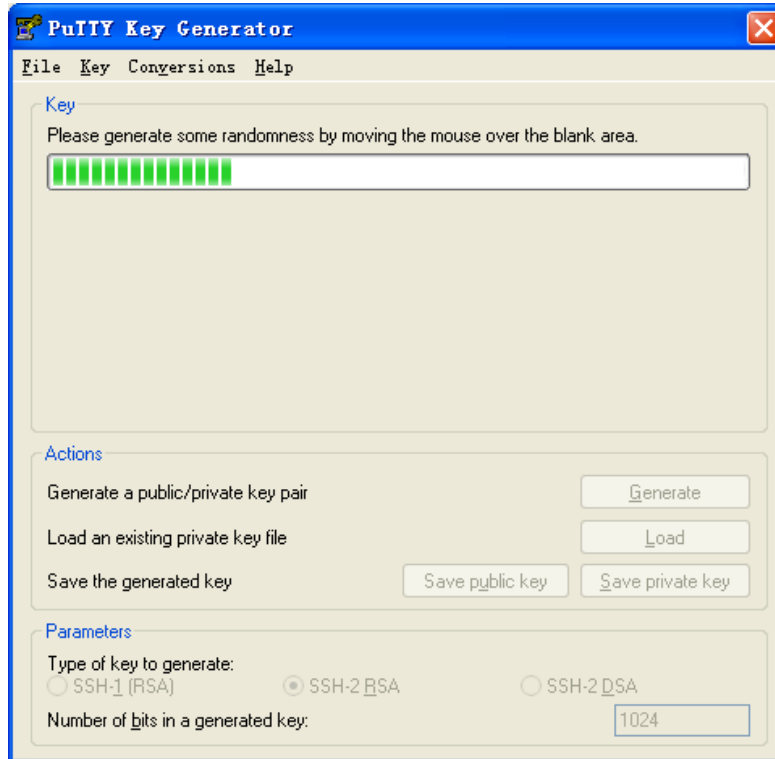
Run PuTTYGen.exe, select **SSH-2 RSA** and click **Generate**.

Figure 61 Generate a key pair on the client 1)



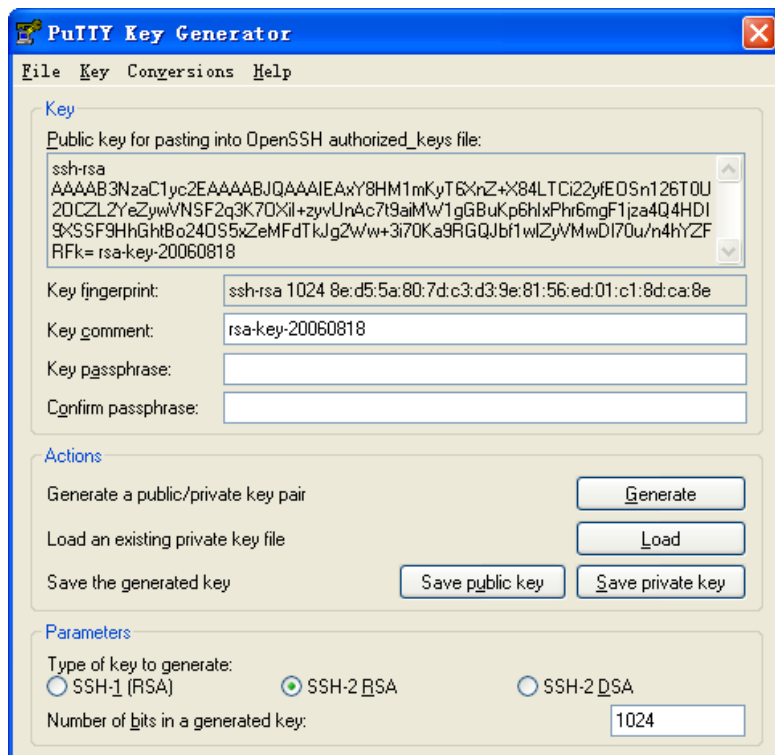
While the key pair is being generated, you must move the mouse continuously and keep the mouse off the green progress bar shown in [Figure 62](#). Otherwise, the progress bar stops moving and the key pair generating process will be stopped.

Figure 62 Generate a key pair on the client 2)



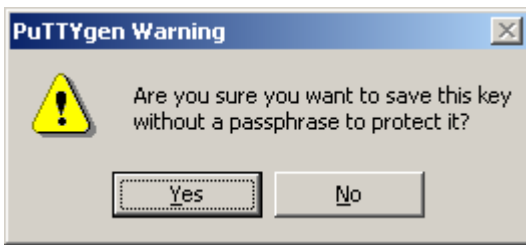
After the key pair is generated, click **Save public key** and specify the file name as **key.pub** to save the public key.

Figure 63 Generate a key pair on the client 3)



Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any protection. Click **Yes** and enter the name of the file for saving the key—**private** in this case.

Figure 64 Save a key pair on the client 4)



Then, 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 4
```

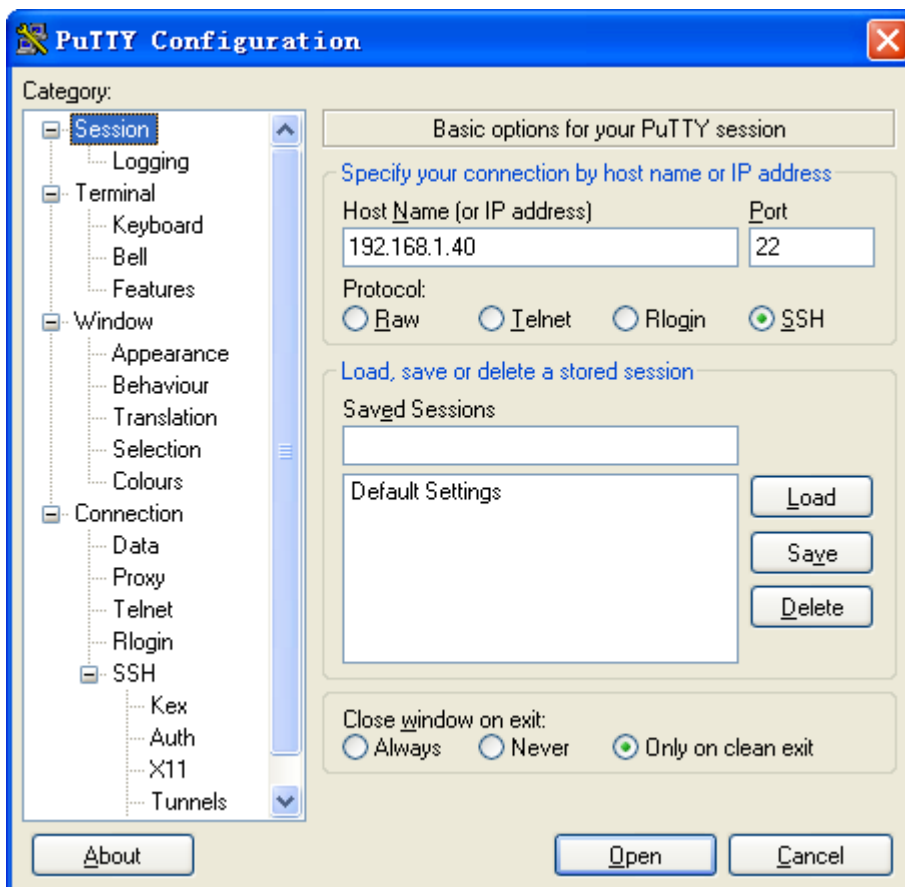
```
[Switch-ui-vty0-4] authentication-mode scheme
# Enable the user interfaces to support SSH.
[Switch-ui-vty0-4] protocol inbound ssh
# Set the user command privilege level to 3.
[Switch-ui-vty0-4] user privilege level 3
[Switch-ui-vty0-4] quit
# Import the client's public key from file key.pub and 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. Establish a connection between the SSH client and the SSH server

Specify the private key file and establish a connection to the SSH server

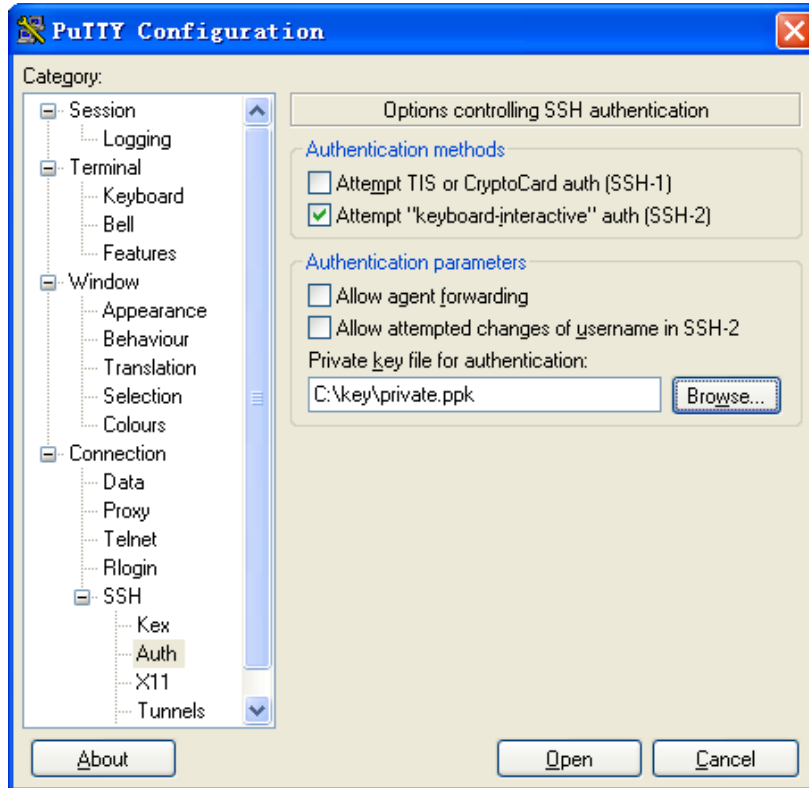
Launch PuTTY.exe to enter the following interface. In the **Host Name or IP address** text box, enter the IP address of the server—192.168.1.40.

Figure 65 SSH client configuration interface 1)



Select **Connection > SSH > Auth** from the navigation tree. The following window appears. Click **Browse...** to bring up the file selection window, navigate to the private key file and click **OK**.

Figure 66 SSH client configuration interface 2)



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.

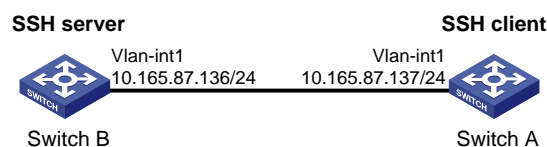
SSH client configuration examples

When switch acts as client for password authentication

Network requirements

As shown in Figure 67, 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 67 Switch acts as client for password authentication



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 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

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

Create local user **client001**.

```
[SwitchB] local-user client001
[SwitchB-luser-client001] password simple aabcc
[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

```

- If the client supports first-time authentication, the client directly establishes a connection with 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, the client logs 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] D716D7DB9FCABB4ADB6FB4FDB0CA25C761B308EF53009F71
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:

```

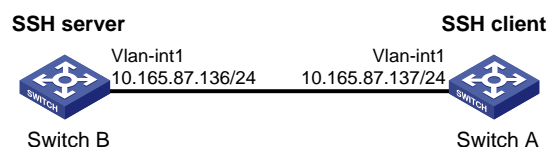
After you enter the correct password, the client logs in to Switch B successfully.

When switch acts as client for publickey authentication

Network requirements

As shown in [Figure 68](#), 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 68 Switch acts as client for publickey authentication



Configuration procedure

NOTE:

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 4
[SwitchB-ui-vty0-4] authentication-mode scheme

```

Enable the user interfaces to support SSH.

```

[SwitchB-ui-vty0-4] protocol inbound ssh

```

Set the user command privilege level to 3.

```
[SwitchB-ui-vty0-4] user privilege level 3  
[SwitchB-ui-vty0-4] 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 a connection between the SSH client and the SSH server

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.

SFTP configuration

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 device can serve as the SFTP server, allowing a remote user to log in to the SFTP server for secure file management and transfer. The device can also server as an SFTP client, enabling a user to login from the device to a remote device for secure file transfer.

Configuring the device as an SFTP server

Configuration prerequisites

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 the chapter “SSH configuration.”

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.

Follow these steps to enable the SFTP server:

| To do... | Use the command... | Remarks |
|------------------------|---------------------------|---------------------------------|
| Enter system view | system-view | — |
| Enable the SFTP server | sftp server enable | Required Disabled by default |

NOTE:

When the device functions as the SFTP server, 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.

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.

Follow these steps to configure the SFTP connection idle timeout period:

| To do... | Use the command... | Remarks |
|---|---|-----------------------------------|
| Enter system view | system-view | — |
| Configure the SFTP connection idle timeout period | sftp server idle-timeout <i>time-out-value</i> | Optional 10 minutes by default |

Configuring the device 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.

Follow these steps to specify a source IP address or interface for the SFTP client:

| To do... | Use the command... | Remarks |
|--|--|--|
| Enter system view | system-view | — |
| 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 <i>ip-address</i> interface <i>interface-type interface-number</i> } | Required Use either command. By default, an SFTP client uses the IP address of the interface specified by the route of the device to access the SFTP server. |
| Specify a source IPv6 address or interface for the SFTP client | Specify a source IPv6 address or interface for the SFTP client sftp client ipv6 source { ipv6 <i>ipv6-address</i> interface <i>interface-type interface-number</i> } | |

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.

Follow these steps to enable the SFTP client:

| To do... | Use the command... | Remarks |
|---|---|--|
| Establish a connection to the remote SFTP server and enter SFTP client view | Establish a connection to the remote IPv4 SFTP server and enter SFTP client view sftp server [<i>port-number</i>] [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 }] * | Required Use either command in user view. |

| To do... | Use the command... | Remarks |
|--|--|---------|
| Establish a connection to the remote IPv6 SFTP server and enter SFTP client view | sftp ipv6 server [<i>port-number</i>] [identity-key { <i>dsa</i> <i>rsa</i> } prefer-ctos-cipher { <i>3des</i> <i>aes128</i> <i>des</i> } prefer-ctos-hmac { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> } prefer-kex { <i>dh-group-exchange</i> <i>dh-group1</i> <i>dh-group14</i> } prefer-stoc-cipher { <i>3des</i> <i>aes128</i> <i>des</i> } prefer-stoc-hmac { <i>md5</i> <i>md5-96</i> <i>sha1</i> <i>sha1-96</i> }] * | |

Working with SFTP directories

SFTP directory operations include:

- Changing or displaying the current working directory
- Displaying files under a specified directory or the directory information
- Changing the name of a specified directory on the server
- Creating or deleting a directory

Follow these steps to work with the SFTP directories:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter SFTP client view | For more information, see “Establishing a connection to the SFTP server.” | Required Execute the command in user view. |
| Change the working directory of the remote SFTP server | cd [<i>remote-path</i>] | Optional |
| Return to the upper-level directory | cdup | Optional |
| Display the current working directory of the remote SFTP server | pwd | Optional |
| Display files under a specified directory | dir [-a -l] [<i>remote-path</i>] ls [-a -l] [<i>remote-path</i>] | Optional The dir command functions as the ls command. |
| Change the name of a specified directory on the SFTP server | rename <i>oldname newname</i> | Optional |
| Create a new directory on the remote SFTP server | mkdir <i>remote-path</i> | Optional |
| Delete one or more directories from the SFTP server | rmdir <i>remote-path</i> &<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

Follow these steps to work with SFTP files:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter SFTP client view | For more information, see "Establishing a connection to the SFTP server." | Required Execute the command in user view. |
| Change the name of a specified file or directory on the SFTP server | rename <i>old-name new-name</i> | Optional |
| Download a file from the remote server and save it locally | get <i>remote-file [local-file]</i> | Optional |
| Upload a local file to the remote SFTP server | put <i>local-file [remote-file]</i> | Optional |
| Display the files under a specified directory | dir [-a -l] [<i>remote-path</i>] ls [-a -l] [<i>remote-path</i>] | Optional The dir command functions as the ls command. |
| Delete one or more directories from the SFTP server | delete <i>remote-file&<1-10></i> remove <i>remote-file&<1-10></i> | 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.

Follow these steps to display a list of all commands or the help information of an SFTP client command:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter SFTP client view | For more information, see "Establishing a connection to the SFTP server." | Required Execute the command in user view. |
| Display a list of all commands or the help information of an SFTP client command | help [all <i>command-name</i>] | Required |

Terminating the connection to the remote SFTP server

Follow these steps to terminate the connection to the remote SFTP server:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter SFTP client view | For more information, see "Establishing a connection to the SFTP server." | Required Execute the command in user view. |
| Terminate the connection to the remote SFTP server and return to | bye exit | Required Use any of the commands. |

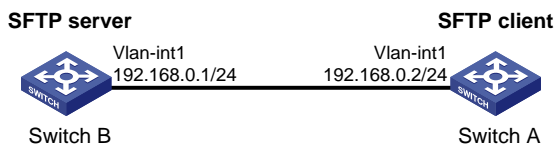
| To do... | Use the command... | Remarks |
|-----------|--------------------|--|
| user view | quit | These three commands function in the same way. |

SFTP client configuration example

Network requirements

As shown in [Figure 69](#), an SSH connection is established between Switch A and Switch B. Switch A, an SFTP client, logs in to Switch B for file management and file transfer. An SSH user uses publickey authentication with the public key algorithm being RSA.

Figure 69 Network diagram for SFTP client configuration



Configuration procedure

NOTE:

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 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

Set the protocol that a remote user uses to log in as SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] 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.
```

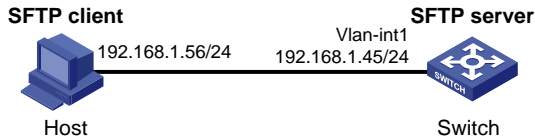
```
<SwitchA>
```

SFTP server configuration example

Network requirements

As shown in [Figure 70](#), an SSH connection is established between the host and the switch. The host, an SFTP client, logs in to the switch for file management and file transfer. An SSH user uses password authentication with the username **client002** and the password **aabbcc**. The username and password are saved on the switch.

Figure 70 Network diagram for SFTP server configuration



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 4
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

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

NOTE:

- The device support many types of SFTP client software. The following uses PSFTP of PuTTY Version 0.58 as an example.
 - PSFTP supports only password authentication.
-

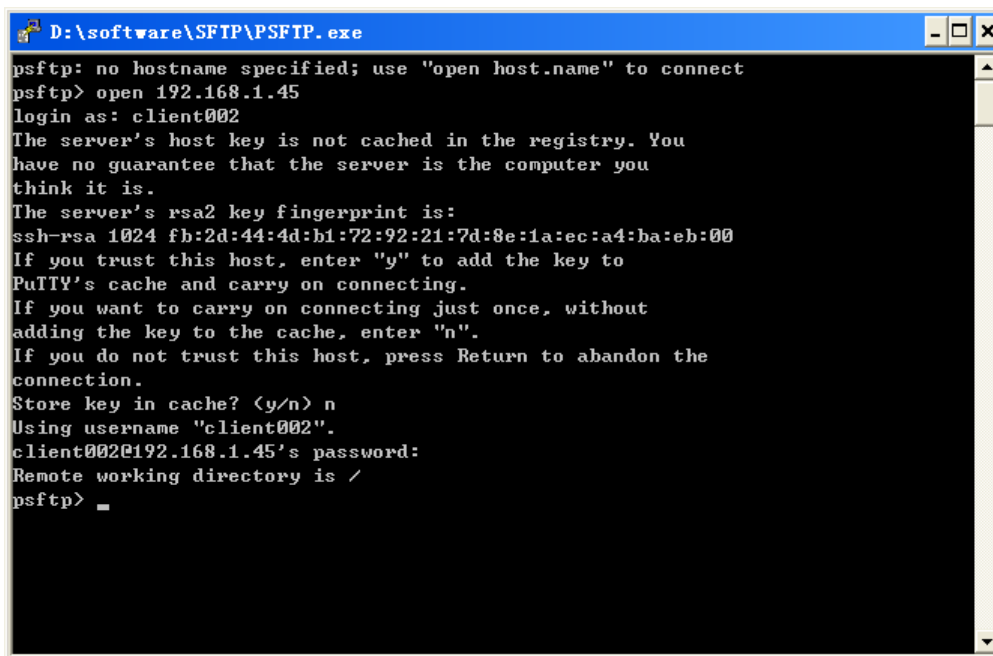
Establish a connection to the remote SFTP server.

Run the psftp.exe to launch the client interface as shown in [Figure 71](#), and enter the following command:

```
open 192.168.1.45
```

Enter username **client002** and password **aabbcc** as prompted to log in to the SFTP server.

Figure 71 SFTP client interface



```
D:\software\SFTP\PSFTP.exe
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> _
```

SSL configuration

SSL overview

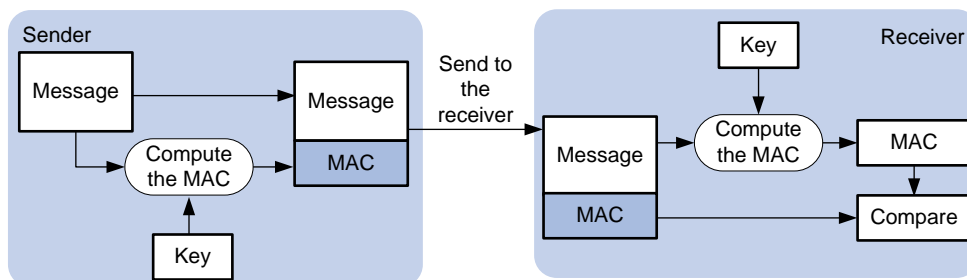
Secure Sockets Layer (SSL) is a security protocol that provides secure connection services for TCP-based application layer protocols, such as HTTP. It is widely used in E-business and online banking to ensure secure data transmission over the Internet.

SSL security mechanism

Secure connections provided by SSL have these features:

- Confidentiality—SSL uses a symmetric encryption algorithm to encrypt data and uses the asymmetric key 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 72 Message integrity verification by a MAC algorithm



NOTE:

- For more information about symmetric key algorithms, asymmetric key algorithm RSA and digital signature, see the chapter "Public key configuration."
 - For more information about PKI, certificate, and CA, see the chapter "PKI configuration."
-

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 73 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—A very important part of the SSL protocol stack, responsible for negotiating the cipher suite to be used for secure communication (including the symmetric encryption algorithm, key exchange algorithm, and MAC algorithm), securely exchanging the key between the server and client, and implementing 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.

SSL configuration task list

Complete the following tasks to configure SSL:

| 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 layer protocol such as HTTP.

Configuration prerequisites

Configure the PKI domain for the SSL server policy to use to obtain the server side certificate. For more information about PKI domain configuration, see the chapter “PKI configuration.”

Configuration procedure

Follow these steps to configure an SSL server policy:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Create an SSL server policy and enter its view | ssl server-policy <i>policy-name</i> | Required |
| Specify a PKI domain for the SSL server policy | pki-domain <i>domain-name</i> | Required By default, no PKI domain is specified for an SSL server policy. |
| Specify the cipher suite(s) for the SSL server policy to support | ciphersuite [rsa_3des_edc_cbc_sha rsa_aes_128_cbc_sha rsa_aes_256_cbc_sha rsa_des_cbc_sha rsa_rc4_128_md5 rsa_rc4_128_sha] * | Optional By default, an SSL server policy supports all cipher suites. |
| Set the handshake timeout time for the SSL server | handshake timeout <i>time</i> | Optional 3,600 seconds by default |
| Set the SSL connection close mode | close-mode wait | Optional Not wait by default |
| Set the maximum number of cached sessions and the caching timeout time | session { cache-size <i>size</i> timeout <i>time</i> } * | Optional The defaults are as follows: <ul style="list-style-type: none"> • 500 for the maximum number of cached sessions, • 3600 seconds for the caching timeout time. |
| Enable certificate-based SSL client authentication | client-verify enable | Optional Not enabled by default |

NOTE:

- If you enable client authentication here, you must request a local certificate for the client.
- 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 device acts as an SSL server, it can communicate with clients running SSL 3.0 or TLS 1.0, and can identify Hello packets from clients running SSL 2.0. If a client running SSL 2.0 also supports SSL 3.0 or TLS 1.0 (information about supported versions is carried in the packet that the client sends to the server), the server will notify the client to use SSL 3.0 or TLS 1.0 to communicate with the server.

SSL server policy configuration example

Network requirements

As shown in [Figure 74](#), users can access and control the device through web pages. For security of the device, users must use HTTPS (HTTP Secure, which uses SSL) to log in to the web interface of the device and use SSL for identity authentication to ensure that data will not be eavesdropped or tampered with.

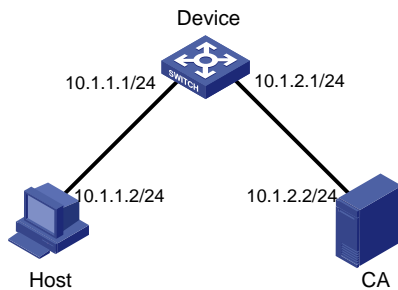
To achieve the goal, perform the following configurations:

- 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.

NOTE:

- 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, ensure that the device, the host, and the CA server can reach each other.
-

Figure 74 Network diagram for SSL server policy configuration



Configuration procedure

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 telnet.
[Device] local-user usera
[Device-luser-usera] password simple 123
[Device-luser-usera] service-type telnet

```

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 device 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 device.

NOTE:

- For more information about PKI configuration commands and the **public-key local create rsa** command, see the *Security Command Reference*.
 - For more information about HTTPS, see the *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.

Configuration prerequisites

If the SSL server is configured to authenticate the SSL client, you must configure the PKI domain for the SSL client policy to use to obtain the certificate of the client. For more information about PKI domain configuration, see the chapter “PKI configuration.”

Configuration procedure

Follow these steps to configure an SSL client policy:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|--|---|---|
| Create an SSL client policy and enter its view | ssl client-policy <i>policy-name</i> | Required |
| Specify a PKI domain for the SSL client policy | pki-domain <i>domain-name</i> | Optional No PKI domain is configured by default. |
| Specify the preferred cipher suite for the SSL client policy | prefer-cipher { rsa_3des_edc_cbc_sha rsa_aes_128_cbc_sha rsa_aes_256_cbc_sha rsa_des_cbc_sha rsa_rc4_128_md5 rsa_rc4_128_sha } | Optional rsa_rc4_128_md5 by default |
| Specify the SSL protocol version for the SSL client policy | version { ssl3.0 tls1.0 } | Optional TLS 1.0 by default |
| Enable certificate-based SSL server authentication | server-verify enable | Optional Enabled by default |

NOTE:

If you enable client authentication on the server, you must request a local certificate for the client.

Displaying and maintaining SSL

| To do... | Use the command... | Remarks |
|---------------------------------------|---|-----------------------|
| Display SSL server policy information | display ssl server-policy { <i>policy-name</i> all } [[{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display SSL client policy information | display ssl client-policy { <i>policy-name</i> all } [[{ begin exclude include } <i>regular-expression</i>] | |

Troubleshooting SSL

SSL handshake failure

Symptom

As the SSL server, the device 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.

TCP attack protection configuration

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 the 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 the ESTABLISHED state. In this way, incomplete TCP connections could be avoided to protect the server against SYN Flood attacks.

Follow these steps to enable the SYN Cookie feature:

| To do... | Use the command... | Remarks |
|-------------------------------|------------------------------|---------------------------------|
| Enter system view | system-view | — |
| Enable the SYN Cookie feature | tcp syn-cookie enable | Required Enabled by default. |

NOTE:

With the SYN Cookie feature enabled, only the MSS, is negotiated during TCP connection establishment, instead of the window's zoom factor and timestamp.

Displaying and maintaining TCP attack protection

| To do... | Use the command... | Remarks |
|--------------------------------------|--|-----------------------|
| Display current TCP connection state | display tcp status [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

IP source guard configuration

IP source guard overview

Introduction to IP source guard

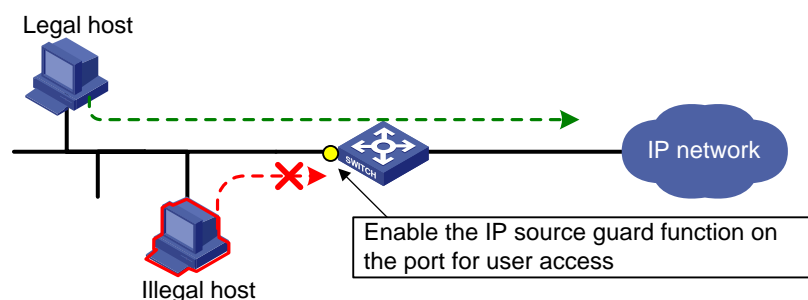
IP source guard is intended to work on a port connecting users. It filters received packets to block illegal access to network resources, improving network security. For example, it can prevent illegal hosts from using a legal IP address to access the network.

IP source guard can filter packets according to the packet source IP address, and source MAC address. It supports these types of binding entries:

- IP-port binding entry
- MAC-port binding entry
- IP-MAC-port binding entry

After receiving a packet, an IP source guard-enabled port obtains the key attributes (source IP address, and source MAC address) of the packet and then looks them up in the binding entries of IP source guard. If there is a match, the port forwards the packet; otherwise, the port discards the packet, as shown in [Figure 75](#). IP source guard binding entries are on a per-port basis. After a binding entry is configured on a port, it is effective only on the port.

Figure 75 Diagram for the IP source guard function



IP source guard binding

An IP source guard binding entry can be static or dynamic.

Static IP source guard binding

A static IP source guard binding entry is configured manually. It is suitable for scenarios where only 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.

1. Types of static IP source guard binding entries

According to the IP version, a static IP source guard binding entry is an IPv4 or IPv6 entry.

- A static IPv4 source guard binding entry filters IPv4 packets received by the port or checks the validity of users by cooperating with the ARP detection feature.
- A static IPv6 source guard binding entry filters IPv6 packets received by the port or checks the validity of users by cooperating with the ND detection feature.

NOTE:

- For information about ARP detection, see the chapter “ARP attack protection configuration.”
 - For information about ND detection, see the chapter “ND attack defense configuration.”
-

2. Validity ranges of static IP source guard binding entries

According to the validity range, a static IP source guard binding entry is a global or port-based static binding entry:

- A global static binding entry is effective on all ports. A port forwards a packet only when the packet’s IP address and MAC address both matches those in a global static binding entry or both do not match those in any global static binding entry. If only the IP address or MAC address of the packet matches that of a global static binding entry, the port discards the packet. Global static binding entries are used to protect against host spoofing attacks. They can effectively filter attack packets that exploit the IP address or MAC address of a legal user host.
- A port-based static binding entry is effective on only the specified port. A port forwards a packet only when the IP address, and MAC address of the packet all match those in a static binding entry on the port. All other packets will be dropped. Port-based static binding entries are used to check the validity of users that are trying to access a port.

NOTE:

Global static IP source guard binding entries take effect on all ports. However, port-based static IP source guard binding entries and dynamic IP source guard binding entries take precedence over global static IP source guard binding entries. If a port is configured with a static binding entry or dynamic binding, the global static binding entries do not take effect on the port.

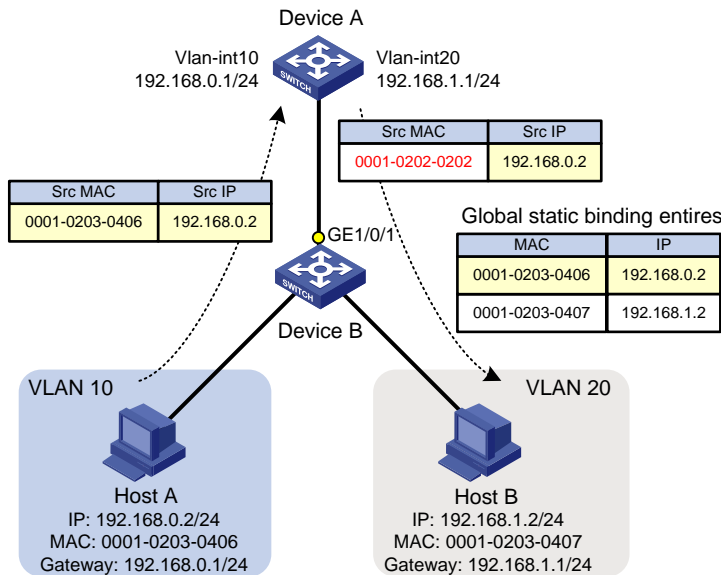
3. Excluded ports of global static binding entries

In some circumstances, global static binding entries may result in communication failures on some ports. In such cases, specify the ports as excluded ports, so that global static binding entries do not take effect on these ports.

As shown in [Figure 77](#), Device B is an access layer device connected to hosts of different VLANs. Device A works at the distribution layer as a gateway to allow hosts in different VLANs to communicate at Layer 3. When a host in a VLAN communicates with a host in another VLAN, Device A forwards IP packets between the VLANs, changing the source MAC addresses of the IP packets. For example, when Device A receives an IP packet from Host A to Host B, it changes the source MAC address of the IP packet from 0001-0203-0406 to 0001-0202-0202, its own MAC address. If you configure a global static binding entry with Host A’s IP address and MAC address, Device B will drop the packets because the packets’ IP address matches the entry but their source MAC address does not match the entry, preventing hosts in different VLANs from communicating at Layer 3.

To solve the problem, specify the uplink port (GE1/0/1) of Device B as an excluded port for global static binding. Then, the global static binding entry does not take effect on the uplink port, and packets forwarded by Device A will be forwarded normally.

Figure 76 Network diagram for excluded port application in IP source guard global static binding



NOTE:

After you configure IPv4 or IPv6 global static binding entries on a switch, configure the uplink port of the switch as an excluded port of global static binding to ensure packet forwarding between VLANs.

Dynamic IP source guard binding

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 binding generates IPv4 source guard binding entries dynamically based on DHCP snooping or DHCP relay entries to filter IPv4 packets received on a port.
- Dynamic IPv6 source guard binding generates IPv6 source guard binding entries dynamically based on DHCPv6 snooping or ND snooping entries to filter IPv6 packets received on a port.

NOTE:

- For information about DHCP snooping and DHCP relay, see the *Layer 3—IP Services Configuration Guide*.
- For information about DHCPv6 snooping, see the *Layer 3—IP Services Configuration Guide*.
- For information about ND snooping, see the *Layer 3—IP Services Configuration Guide*.

Configuring IPv4 source guard binding

NOTE:

You cannot configure the IP source guard function on a port in an aggregation group, nor can you add a port configured with IP source guard to an aggregation group.

Configuring a static IPv4 source guard binding entry

Follow these steps to configure a global static IPv4 source guard entry:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Configure a global static IPv4 source guard binding entry | user-bind ip-address <i>ip-address</i> mac-address <i>mac-address</i> | Required No global static binding entry exists by default. |
| Enter Layer 2 Ethernet port view | interface <i>interface-type interface-number</i> | — |
| Specify the uplink port as an excluded port of the global static binding entry | user-bind uplink | Optional By default, a port is not an excluded port. When you configure global static binding entries on a switch, specify the uplink port of the switch as an excluded port of the global static binding entries. |

Follow these steps to configure a port-based static IPv4 source guard binding entry:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Configure a static IPv4 source guard binding entry for the port | user-bind { ip-address <i>ip-address</i> ip-address <i>ip-address</i> mac-address <i>mac-address</i> mac-address <i>mac-address</i> } [vlan <i>vlan-id</i>] | Required No static IPv4 source guard binding entry exists on a port by default. The switch does not support the vlan <i>vlan-id</i> option. |

NOTE:

- You cannot configure the same static binding entry on one port for multiple times, but you can configure the same static entry on different ports.
- In an IPv4 source guard binding entry, the MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address, and the IPv4 address can only be a Class A, Class B, or Class C address and can be neither 127.x.x.x nor 0.0.0.0.

Configuring the dynamic IPv4 source guard binding function

After the dynamic IPv4 source guard binding function is enabled on a port, IP source guard will generate binding entries dynamically through cooperation with DHCP protocols:

- 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.

Follow these steps to configure the dynamic IPv4 source guard binding function:

| To do... | Use the command... | Remarks |
|--|---|---------------------------------------|
| Enter system view | system-view | — |
| Enter interface view | interface <i>interface-type interface-number</i> | — |
| Configure the dynamic IPv4 source guard binding function | ip check source { ip-address ip-address mac-address mac-address } | Required Not configured by default |

NOTE:

- To implement dynamic IPv4 source guard binding in IP source guard, make sure that DHCP snooping or DHCP relay is configured and works normally. For DHCP configuration information, see the *Layer 3—IP Services Configuration Guide*.
- If you configure dynamic IPv4 source guard binding on a port for multiple times, the last configuration will overwrite the previous configuration on the port.

Configuring IPv6 source guard binding

NOTE:

You cannot configure the IP source guard function on a port in an aggregation group, nor can you add a port configured with IP source guard to an aggregation group.

Configuring a static IPv6 source guard binding entry

Follow these steps to configure a global static IPv6 source guard entry:

| To do... | Use the command... | Remarks |
|---|---|---|
| Enter system view | system-view | — |
| Configure a global static IPv6 source guard binding entry | user-bind ipv6 ip-address <i>ip-address</i> mac-address <i>mac-address</i> | Required No global static binding entry exists by default. |
| Enter Layer 2 Ethernet port view | interface <i>interface-type interface-number</i> | — |

| To do... | Use the command... | Remarks |
|--|-------------------------|---|
| Specify the uplink port as an excluded port of the global static binding entry | user-bind uplink | Optional By default, a port is not an excluded port. When you configure global static binding entries on a switch, specify the uplink port of the switch as an excluded port of the global static binding entries. |

Follow the steps to configure a port-based static IPv6 source guard binding entry:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet interface view | interface <i>interface-type interface-number</i> | — |
| Configure a static IPv6 source guard binding entry for the port | user-bind ipv6 { ip-address <i>ipv6-address</i> ip-address <i>ipv6-address</i> mac-address <i>mac-address</i> mac-address <i>mac-address</i> } [vlan <i>vlan-id</i>] | Required No static IPv6 source guard binding entry exists on a port by default. The switch does not support the vlan <i>vlan-id</i> option. |

NOTE:

- 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 binding 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.

Configuring the dynamic IPv6 source guard binding function

With the dynamic IPv6 source guard binding function enabled on a Layer 2 port, IP source guard dynamically generates IP source guard entries through cooperation with DHCP snooping or ND snooping.

- 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.

Follow these steps to configure the dynamic IPv6 source guard binding function:

| To do... | Use the command... | Remarks |
|--|--|---------------------------------------|
| Enter system view | system-view | — |
| Enter interface view | interface <i>interface-type interface-number</i> | — |
| Configure dynamic IPv6 source guard binding function | ip check source ipv6 { ip-address ip-address mac-address mac-address } | Required Not configured by default |

NOTE:

- To implement dynamic IPv6 source guard binding, make sure that DHCPv6 snooping or ND snooping is configured and works normally. For DHCPv6 and ND snooping configuration information, see the *Layer 3—IP Services Configuration Guide*.
- If you configure dynamic IPv6 source guard binding on a port for multiple times, the last configuration will overwrite the previous configuration on the port.
- If you configure both ND snooping and DHCPv6 snooping on the device, IP source guard generates IP source guard entries based on the DHCPv6 snooping entries, which are usually generated first, to filter packets on a port.

Displaying and maintaining IP source guard

For IPv4:

| To do... | Use the command... | Remarks |
|---|--|-----------------------|
| Display static IP source guard binding entries | display user-bind [interface <i>interface-type interface-number</i> ip-address <i>ip-address</i> mac-address <i>mac-address</i>] [slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |
| Display dynamic IP source guard binding entries | display ip check source [interface <i>interface-type interface-number</i> ip-address <i>ip-address</i> mac-address <i>mac-address</i>] [slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |

For IPv6:

| To do... | Use the command... | Remarks |
|---|---|-----------------------|
| Display static IPv6 source guard binding entries | display user-bind ipv6 [interface <i>interface-type interface-number</i> ip-address <i>ip-address</i> mac-address <i>mac-address</i>] [slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |
| Display dynamic IPv6 source guard binding entries | display ip check source ipv6 [interface <i>interface-type interface-number</i> ip-address <i>ip-address</i> mac-address <i>mac-address</i>] [slot <i>slot-number</i>] [[{ begin exclude include } <i>regular-expression</i>]] | Available in any view |

IP source guard configuration examples

Static IPv4 source guard binding entry configuration example

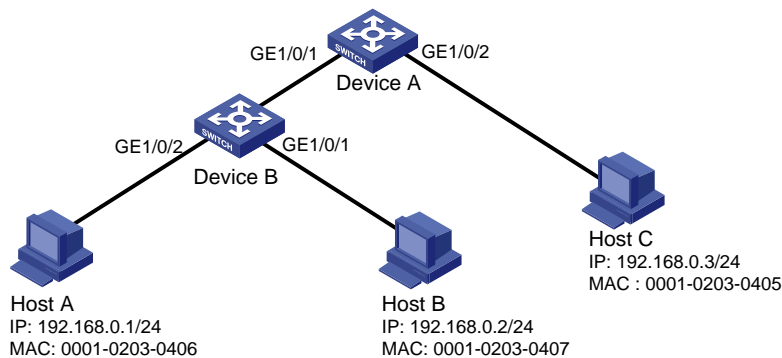
Network requirements

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.

Configure static IPv4 source guard binding 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 from Host B can pass.

Figure 77 Network diagram for configuring static IPv4 source guard binding entries



Configuration procedure

1. Configure Device A

Configure the IP addresses of the interfaces (omitted).

Configure port GigabitEthernet 1/0/2 of Device A 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> system-view
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] user-bind ip-address 192.168.0.3 mac-address 0001-0203-0405
[DeviceA-GigabitEthernet1/0/2] quit
```

Configure port GigabitEthernet 1/0/1 of Device A 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] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.1 mac-address 0001-0203-0406
```

2. Configure Device B

Configure the IP addresses of the interfaces (omitted).

Configure port GigabitEthernet 1/0/2 of Device B 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> system-view
[DeviceB] interface gigabitethernet 1/2
[DeviceB-GigabitEthernet1/0/2] user-bind ip-address 192.168.0.1 mac-address 0001-0203-0406
[DeviceB-GigabitEthernet1/0/2] quit
```

Configure port GigabitEthernet 1/0/1 of Device B to allow only IP packets with the source MAC address of 0001-0203-0407 and the source IP address of 192.168.0.2 to pass.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.2 mac-address 0001-0203-0407
```

Verification

On Device A, display information about static IPv4 source guard binding entries. The output shows that the static IPv4 source guard binding entries are configured successfully.

```
<DeviceA> display user-bind
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 binding entries. The output shows that the static IPv4 source guard binding entries are configured successfully.

```
<DeviceB> display user-bind
Total entries found: 2
  MAC Address      IP Address      VLAN   Interface      Type
  -----
  0001-0203-0406   192.168.0.1    N/A    GE1/0/2        Static
  0001-0203-0407   192.168.0.2    N/A    GE1/0/1        Static
```

Global static binding excluded port configuration example

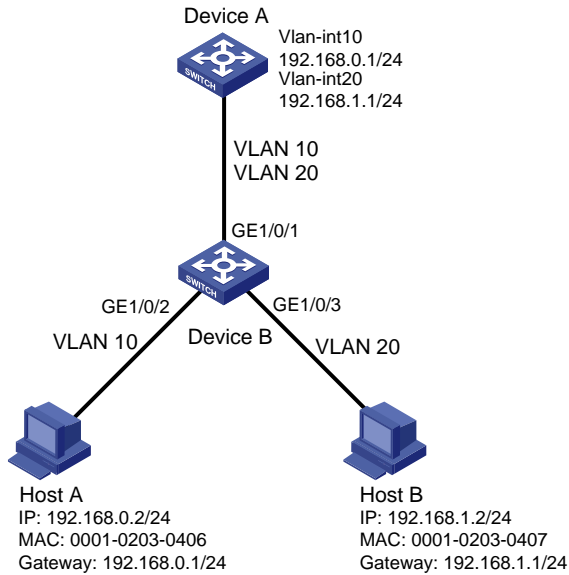
Network requirements

As shown in [Figure 78](#), Host A and Host B connect to access switch Device B, and Device B connects to distribution switch Device A. Host A is in VLAN 10, and its gateway IP address is 192.168.0.1, which is the IP address of VLAN interface 1 on Device A. Host B is in VLAN 20, and its gateway IP address is 192.168.1.1, which is the IP address of VLAN interface 2 on Device A. Device B has VLANs but not IP addresses configured. Host A and Host B communicate with each other through Device A.

Configure Device B to satisfy the following requirements:

- Device B can filter IP packets from any host that spoofs Host A or Host B.
- Device B forwards packets between Host A and Host B.

Figure 78 Network diagram for configuring global static binding excluded port



Configuration procedure

Configure Device B

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
```

Specify port GigabitEthernet 1/0/1 as a trunk port, and configure the port to permit the packets of VLAN 10 and VLAN 20 to pass.

```
[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 global static bindings to filter IP packets from any host spoofs Host A or Host B by using the IP or MAC address of Host A or Host B.

```
<DeviceB> system-view  
[DeviceB] user-bind ip-address 192.168.0.2 mac-address 0001-0203-0406  
[DeviceB] user-bind ip-address 192.168.1.2 mac-address 0001-0203-0407
```

Specify GigabitEthernet 1/0/1 as a global static binding excluded port.

```
[DeviceB] interface gigabitethernet 1/0/1  
[DeviceB-GigabitEthernet1/0/1] user-bind uplink  
[DeviceB-GigabitEthernet1/0/1] quit
```

Verify the configuration

Display the IP source guard bindings on Device B.

```
[DeviceB] display user-bind
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
```

Host A and Host B can ping each other.

Dynamic IPv4 source guard binding by DHCP snooping configuration example

Network requirements

As shown in [Figure 79](#), the device connects to the host (client) and the DHCP server through ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 respectively.

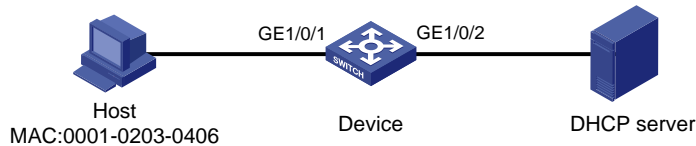
Enable DHCP and DHCP snooping on the device, so that the host (with the MAC address of 0001-0203-0406) can obtain an IP address through the DHCP server and the IP address and the MAC address of the host can be recorded in a DHCP snooping entry.

Enable the dynamic IPv4 source guard binding function on port GigabitEthernet 1/0/1 of the device, allowing only packets from a client that obtains an IP address through the DHCP server to pass.

NOTE:

For detailed configuration of a DHCP server, see the *Layer 3—IP Services Configuration Guide*.

Figure 79 Network diagram for configuring dynamic IPv4 source guard binding by DHCP snooping



Configuration procedure

1. Configure DHCP snooping

Configure IP addresses for the interfaces. (details not shown)

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 dynamic IPv4 source guard binding function

Configure the dynamic IPv4 source guard binding 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 check source ip-address mac-address
```

```
[Device-GigabitEthernet1/0/1] quit
```

Verification

Display the dynamic IPv4 source guard binding entries generated on port GigabitEthernet 1/0/1.

```
[Device-GigabitEthernet1/0/1] display ip check source
```

```
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-GigabitEthernet1/0/1] display dhcp-snooping
```

```
DHCP Snooping is enabled.
```

```
The client binding table for all untrusted ports.
```

```
Type : D--Dynamic , S--Static
```

| Type | IP Address | MAC Address | Lease | VLAN | Interface |
|------|-------------|----------------|-------|------|----------------------|
| D | 192.168.0.1 | 0001-0203-0406 | 86335 | 1 | GigabitEthernet1/0/1 |

The output shows that a dynamic IPv4 source guard entry has been generated based on the DHCP snooping entry.

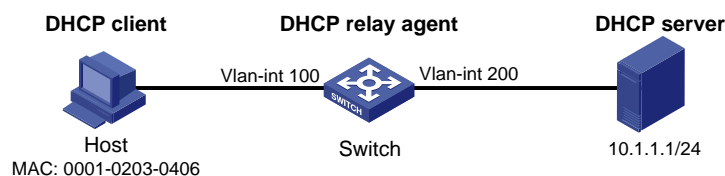
Dynamic IPv4 source guard binding by DHCP relay configuration example

Network requirements

As shown in [Figure 80](#), the switch connects the host and the DHCP server through interfaces VLAN-interface 100 and VLAN-interface 200 respectively. DHCP relay is enabled on the switch. The host (with the MAC address 0001-0203-0406) obtains an IP address from the DHCP server through the DHCP relay agent.

Enable the dynamic IPv4 source guard binding function on interface VLAN-interface 100 to filter packets based on DHCP relay entries.

Figure 80 Network diagram for configuring dynamic IPv4 source guard binding through DHCP relay



Configuration procedure

1. Configure the dynamic IPv4 source guard binding function

Configure the IP addresses of the interfaces. (details not shown)

Configure the dynamic IPv4 source guard binding 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 check source ip-address mac-address
[Switch-Vlan-interface100] quit
```

2. Configure DHCP relay

Enable DHCP relay.

```
[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 work 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
```

Verification

Display the generated dynamic IPv4 source guard binding entries.

```
[Switch] display ip check source
```

Total entries found: 1

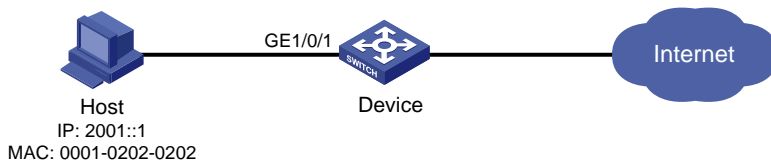
| MAC Address | IP Address | VLAN | Interface | Type |
|----------------|-------------|------|-----------|----------|
| 0001-0203-0406 | 192.168.0.1 | 100 | Vlan100 | DHCP-RLY |

Static IPv6 source guard binding entry configuration example

Network requirements

As shown in [Figure 81](#), the host is connected to port GigabitEthernet 1/0/1 of the device. Configure a static IPv6 source guard binding entry for GigabitEthernet 1/0/1 of the device to allow only packets from the host to pass.

Figure 81 Network diagram for configuring static IPv6 source guard binding entries



Configuration procedure

Configure port 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> system-view
```

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] user-bind ipv6 ip-address 2001::1 mac-address 0001-0202-0202
```

```
[Device-GigabitEthernet1/0/1] quit
```

Verification

On the device, display the information about static IPv6 source guard binding entries. The output shows that the binding entry is configured successfully.

```
[Device] display user-bind ipv6
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 binding by DHCPv6 snooping configuration example

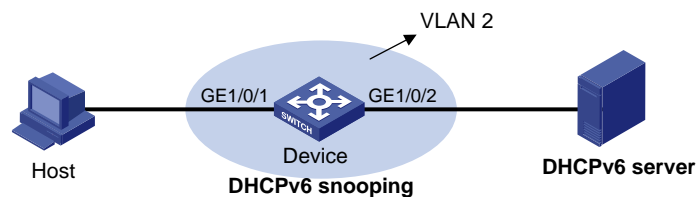
Network requirements

As shown in [Figure 82](#), the device connects to the host (DHCPv6 client) and the DHCPv6 server 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 dynamic IPv6 source guard binding function on port GigabitEthernet 1/0/1 of the device 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 82 Network diagram for configuring dynamic IPv6 source guard binding by DHCPv6 snooping



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 dynamic IPv6 source guard binding function

Configure dynamic IPv6 source guard binding of packet source IP address and MAC address on GigabitEthernet 1/0/1 to filter packets based on the dynamically generated DHCPv6 snooping entries.


```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip check source ipv6 ip-address mac-address
[Device-GigabitEthernet1/0/1] quit
```

Verification

Display the dynamic IPv6 source guard binding entries generated on port GigabitEthernet 1/0/1.

```
[Device] display ip check source ipv6
```

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 binding by ND snooping configuration example

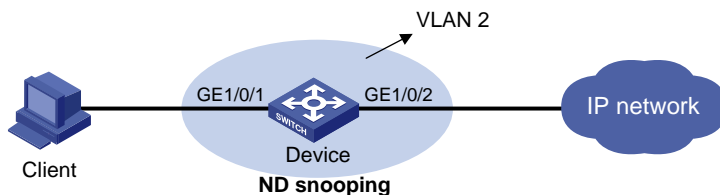
Network requirements

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 dynamic IPv6 source guard binding function on port GigabitEthernet 1/0/1 to filter packets based on ND snooping entries, allowing only packets with a legally obtained IPv6 address to pass.

Figure 83 Network diagram for configuring dynamic IPv6 source guard binding by ND snooping



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 dynamic IPv6 source guard binding function.

Configure dynamic IPv6 source guard binding of packet source IP address and MAC address on GigabitEthernet 1/0/1 to filter packets based on the dynamically generated ND snooping entries.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip check source ipv6 ip-address mac-address
[Device-GigabitEthernet1/0/1] quit
```

Verification

Display the dynamic IPv6 source guard binding entries generated on port GigabitEthernet 1/0/1.

```
[Device] display ip check source ipv6
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.

Troubleshooting IP source guard

Neither static binding entries nor the dynamic binding function can be configured

Symptom

Failed to configure static binding entries or dynamic binding 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.

ARP attack protection configuration

ARP attack protection overview

Although ARP is easy to implement, it provides no security mechanism and is prone to network attacks. An attacker may send the following:

- ARP packets by acting as a trusted user or gateway so that the receiving devices obtain incorrect ARP entries. As a result, network attacks occur.
- A large number of IP packets with unreachable destinations. As a result, the receiving device continuously resolves destination IP addresses and its CPU is overloaded.
- A large number of ARP packets to create a great impact to the CPU.

For more information about ARP attack features and types, see ARP Attack Protection Technology White Paper.

ARP attacks and viruses threaten LAN security. The switch can provide multiple features to detect and prevent such attacks. This chapter mainly introduces these features.

ARP attack protection configuration task list

Complete the following tasks to configure ARP attack protection:

| Task | Remarks |
|--------------------------------------|--|
| Flood prevention | Configuring ARP source suppression Optional Configure this function on gateways (recommended). |
| | Configuring ARP defense against IP packet attacks 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). |
| User and gateway spoofing prevention | Configuring source MAC address based ARP attack detection Optional Configure this function on gateways (recommended). |
| | 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). |

| Task | Remarks |
|--|--|
| Configuring ARP detection | Optional Configure this function on access devices (recommended). |
| 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

Introduction

If the switch receives a large number of IP packets from a host addressed to unreachable destinations,

- The switch sends a large number of ARP requests to the destination subnets, and thus the load of the destination subnets increases.
- The switch keeps trying to resolve destination IP addresses, which increases the load on the CPU.

To protect the switch 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, whenever the number of ARP requests triggered by the packets with unresolvable destination IP addresses from a host within five seconds exceeds a specified threshold, the switch suppresses the packets of the sending host from triggering any ARP requests within the following five 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 switch 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

Follow these steps to configure ARP source suppression:

| To do... | Use the command... | Remarks |
|-------------------------------|--------------------------------------|----------------------------------|
| Enter system view | system-view | — |
| Enable ARP source suppression | arp source-suppression enable | Required Disabled by default. |

| To do... | Use the command... | Remarks |
|---|---|----------------------------|
| Set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the switch can receive in five consecutive seconds | arp source-suppression limit <i>limit-value</i> | Optional 10 by default. |

Enabling ARP black hole routing

Follow these steps to configure ARP black hole routing:

| To do... | Use the command... | Remarks |
|-------------------------------|-----------------------------------|---------------------------------|
| Enter system view | system-view | — |
| Enable ARP black hole routing | arp resolving-route enable | Optional Enabled by default. |

Displaying and maintaining ARP defense against IP packet attacks

| To do... | Use the command... | Remarks |
|--|--|-----------------------|
| Display the ARP source suppression configuration information | display arp source-suppression [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

Configuring ARP packet rate limit

Introduction

This feature allows you to limit the rate of ARP packets to be delivered to the CPU. For example, if an attacker sends a large number of ARP packets to an ARP detection enabled switch, the CPU of the switch may become overloaded because all of the ARP packets are redirected to the CPU for checking. As a result, the switch fails to deliver other functions properly or even crashes. To prevent this, configure ARP packet rate limit.

Enable this feature after the ARP detection is configured or use this feature to prevent ARP flood attacks.

Configuring ARP packet rate limit

When the ARP packet rate exceeds the rate limit set on an interface, the switch 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 switch will output the peak ARP packet rate in the trap and log messages.

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 switch. 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 the *Network Management and Monitoring Configuration Guide*.

Follow these steps to configure ARP packet rate limit:

| To do... | Use the command... | Remarks |
|--|--|------------------------------------|
| Enter system view | system-view | — |
| Enable ARP packet rate limit trap | snmp-agent trap enable arp rate-limit | Optional Enabled by default. |
| 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. |
| Enter Layer 2 Ethernet port view/Layer 2 aggregate interface view | interface interface-type interface-number | — |
| Configure ARP packet rate limit | arp rate-limit { disable rate pps drop } | Required Disabled by default.. |

NOTE:

- 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.
- For more information about the **snmp-agent trap enable arp rate-limit** command, see the *Network Management and Monitoring Command Reference*.

Configuring source MAC address based ARP attack detection

Introduction

This feature allows the switch to check the source MAC address of ARP packets delivered to the CPU. If the number of ARP packets from a MAC address exceeds a specified threshold within five seconds, the switch considers this an attack and adds the MAC address to the attack detection table. Before the attack detection entry is aged out, the switch generates a log message upon receiving an ARP packet sourced from that MAC address and filters out subsequent ARP packets from that MAC address (in filter mode), or only generates a log message upon receiving an ARP packet sourced from that MAC address (in monitor mode).

A gateway or critical server may send a large number of ARP packets. To prevent these ARP packets from being discarded, you can specify the MAC address of the gateway or server as a protected MAC address. A protected MAC address is excluded from ARP attack detection even if it is an attacker.

Configuration procedure

Follow these steps to configure source MAC address based ARP attack detection:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Enable source MAC address based ARP attack detection and specify the detection mode | arp anti-attack source-mac { filter monitor } | Required Disabled by default. |
| Configure the threshold | arp anti-attack source-mac threshold <i>threshold-value</i> | Optional 50 by default. |
| Configure the age timer for ARP attack detection entries | arp anti-attack source-mac aging-time <i>time</i> | Optional 300 seconds by default. |
| Configure protected MAC addresses | arp anti-attack source-mac exclude-mac <i>mac-address</i> <1-10> | Optional No protected MAC address is 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

| To do... | Use the command... | Remarks |
|---|---|-----------------------|
| Display attacking MAC addresses detected by source MAC address based ARP attack detection | display arp anti-attack source-mac { slot <i>slot-number</i> interface <i>interface-type interface-number</i> } [{ begin exclude include } <i>regular-expression</i>] | Available in any view |

Configuring ARP packet source MAC address consistency check

Introduction

This feature enables a gateway device to filter out ARP packets with a source MAC address in the Ethernet header different from the sender MAC address in the message body, so that the gateway device can learn correct ARP entries.

Configuration procedure

Follow these steps to enable ARP packet source MAC address consistency check:

| To do... | Use the command... | Remarks |
|-------------------|--------------------|---------|
| Enter system view | system-view | — |

| To do... | Use the command... | Remarks |
|--|---|----------------------------------|
| Enable ARP packet source MAC address consistency check | arp anti-attack valid-check enable | Required 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

Follow these steps to configure ARP active acknowledgement:

| To do... | Use the command... | Remarks |
|--|--|----------------------------------|
| Enter system view | system-view | — |
| Enable the ARP active acknowledgement function | arp anti-attack active-ack enable | Required Disabled by default. |

Configuring ARP detection

Introduction

The ARP detection feature is mainly configured on an access device to allow only the ARP packets of authorized clients to be forwarded and prevent user spoofing and gateway spoofing.

ARP detection includes ARP detection based on static IP source guard binding entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses, ARP detection based on specified objects, and ARP restricted forwarding.

NOTE:

If both the ARP detection based on specified objects and the ARP detection based on static IP source guard binding entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses are enabled, the former one applies first, and then the latter applies.

Enabling ARP detection based on static IP source guard binding Entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses

With this feature enabled, the switch compares the sender IP and MAC addresses of an ARP packet received from the VLAN against the static IP source guard binding entries, DHCP snooping entries, 802.1X security entries, or OUI MAC addresses to prevent spoofing.

After you enable this feature for a VLAN:

1. Upon receiving an ARP packet from an ARP untrusted port, the switch 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 switch compares the ARP packet's sender IP and MAC addresses against the DHCP snooping entries, 802.1X security entries, and OUI MAC addresses.
2. If a match is found in any of the entries, the ARP packet is considered valid and is forwarded. ARP detection based on OUI MAC addresses refers to that if the sender MAC address of the received ARP packet is an OUI MAC address and voice VLAN is enabled, the packet is considered valid.
3. If no match is found, the ARP packet is considered invalid and is discarded.
4. Upon receiving an ARP packet from an ARP trusted port, the switch does not check the ARP packet.

NOTE:

- Static IP source guard binding entries are created by using the **user-bind** command. For more information, see the chapter "IP source guard configuration."
 - Dynamic DHCP snooping entries are automatically generated through the DHCP snooping function. For more information, see the *Layer 3—IP Services Configuration Guide*.
 - 802.1X security entries are generated by the 802.1X function. For more information, see the chapter "802.1X configuration."
 - For more information about voice VLANs and QUI MAC addresses, see the *Layer 2—LAN Switching Configuration Guide*.
-

Follow these steps to enable ARP detection for a VLAN and specify a trusted port:

| To do... | Use the command... | Remarks |
|---|---|--|
| Enter system view | system-view | — |
| Enter VLAN view | vlan <i>vlan-id</i> | — |
| Enable ARP detection for the VLAN | arp detection enable | Required ARP detection based on static IP source guard binding entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses is not enabled by default. |
| Return to system view | quit | — |
| Enter Layer 2 Ethernet port view/Layer 2 aggregate interface view | interface <i>interface-type</i> <i>interface-number</i> | — |

| To do... | Use the command... | Remarks |
|--|----------------------------|---|
| 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. |

NOTE:

- When configuring this feature, you need to configure ARP detection based on at least static IP source guard binding entries, DHCP snooping entries, or 802.1X security entries. Otherwise, all ARP packets received from an ARP untrusted port will be discarded, except the ARP packets with an OUI MAC address as the sender MAC address when voice VLAN is enabled.
- When configuring an IP source guard binding entry, you need to specify the VLAN; otherwise, no ARP packet will pass the ARP detection based on static IP source guard binding entries.

Configuring ARP detection based on specified objects

With this feature configured, the switch permits the ARP packets received from an ARP trusted port to pass directly, and checks the ARP packets received from an ARP untrusted port. You can specify objects in the ARP packets to be detected. The objects involve:

- **src-mac:** Checks whether the sender MAC address of an ARP packet 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 in an ARP packet. Any all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded. With this object specified, the sender and target IP addresses of ARP replies, and the source IP address of ARP requests are checked.

Follow these steps to configure ARP detection based on specified objects:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Enter VLAN view | vlan <i>vlan-id</i> | — |
| Enable ARP detection for the VLAN | arp detection enable | Required Disabled by default. |
| Return to system view | quit | — |
| Specify objects for ARP detection | arp detection validate { dst-mac ip src-mac } * | Required Not specified by default. |
| Enter Layer 2 Ethernet port view/Layer 2 aggregate interface view | interface <i>interface-type interface-number</i> | — |
| 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.

Follow these steps to enable ARP restricted forwarding:

| To do... | Use the command... | Remarks |
|----------------------------------|---|----------------------------------|
| Enter system view | system-view | — |
| Enter VLAN view | vlan <i>vlan-id</i> | — |
| Enable ARP restricted forwarding | arp restricted-forwarding enable | Required Disabled by default. |

Displaying and maintaining ARP detection

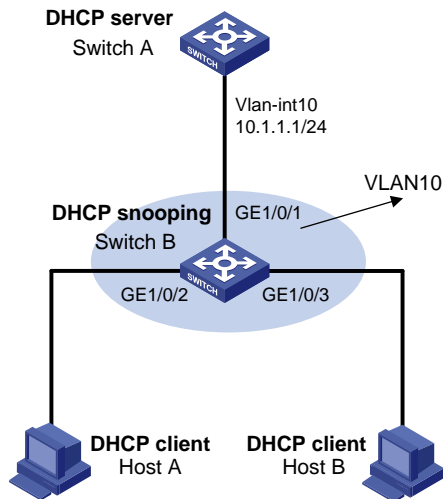
| To do... | Use the command... | Remarks |
|--|--|------------------------|
| Display the VLANs enabled with ARP detection | display arp detection [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display the ARP detection statistics | display arp detection statistics [interface <i>interface-type interface-number</i>] [{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Clear the ARP detection statistics | reset arp detection statistics [interface <i>interface-type interface-number</i>] | Available in user view |

ARP detection configuration example I

Network requirements

As shown in [Figure 84](#), configure Switch A as a DHCP server and enable DHCP snooping on Switch B. Configure Host A as a DHCP client. Configure Host B whose IP address is 10.1.1.6 and MAC address is 0001-0203-0607. Enable ARP detection for VLAN 10 to allow only packets from valid clients or hosts to pass.

Figure 84 Network diagram for ARP detection configuration



Configuration procedure

1. Add all the ports on Switch B to 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 as DHCP client, and Host B as user respectively. (details not shown)

4. Configure Switch B

Enable DHCP snooping.

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] 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 1/0/1
[SwitchB-GigabitEthernet1/0/1] arp detection trust
[SwitchB-GigabitEthernet1/0/1] quit
```

Configure a static IP source guard binding entry on interface GigabitEthernet1/0/3.

```
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] user-bind ip-address 10.1.1.6 mac-address 0001-0203-0607
vlan 10
```

```
[SwitchB-GigabitEthernet1/0/3] quit
```

Enable the checking of the MAC addresses and IP addresses of ARP packets.

```
[SwitchB] arp detection validate dst-mac ip src-mac
```

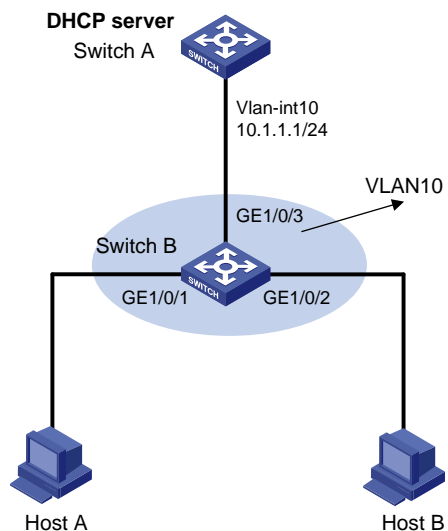
After the preceding configurations are complete, when ARP packets arrive at interfaces GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3, their MAC and IP addresses are checked, and then the packets are checked against the static IP source guard binding entries and finally DHCP snooping entries.

ARP detection configuration example II

Network requirements

As shown in Figure 85, configure Switch A as a DHCP server and Switch B to support 802.1X. Enable ARP detection for VLAN 10 to allow only packets from valid clients to pass. Configure Host A and Host B as local 802.1X access users.

Figure 85 Network diagram for ARP detection configuration



Configuration procedure

1. Add all the 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 (the configuration procedure is omitted) and configure them to upload IP addresses for ARP detection.

4. Configure Switch B

Enable the 802.1X function.

```
<SwitchB> system-view
```

```
[SwitchB] dot1x
```

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-Gigabitethernet 1/0/1] dot1x
[SwitchB-Gigabitethernet 1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-Gigabitethernet 1/0/2] dot1x
[SwitchB-Gigabitethernet 1/0/2] 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.

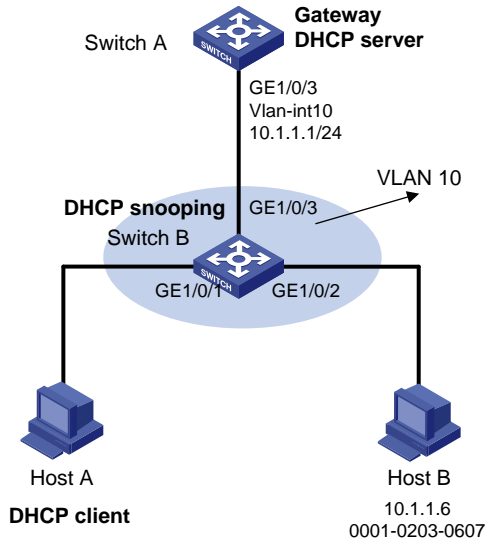
ARP restricted forwarding configuration example

Network requirements

As shown in [Figure 86](#), Switch A acts as a DHCP server. Host A acts as a DHCP client. Host B's IP address is 10.1.1.6, and its MAC address is 0001-0203-0607. Port isolation configured on Switch B isolates the two hosts at Layer 2, which can communicate with the gateway Switch A. GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 belong to VLAN 10. Switch B is enabled with DHCP snooping, and has ARP detection enabled in VLAN 10.

Configure Switch B to still perform port isolation on ARP broadcast requests.

Figure 86 Network diagram for ARP restricted forwarding configuration



Configuration procedure

1. Configure VLAN 10, add ports to VLAN 10, and configure the IP address of the VLAN-interface, as shown in Figure 86. (details not shown)
2. Configure the DHCP server on Switch A.

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 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] user-bind 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, when ARP packets arrive at interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, their MAC and IP addresses are checked, and then the packets 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. Port isolation fails.

Configure ARP restricted forwarding.

```
[SwitchB] vlan 10
```

```
[SwitchB-vlan10] arp restricted-forwarding enable
```

```
[SwitchB-vlan10] quit
```

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

Introduction

ARP automatic scanning is usually used together with the fixed ARP feature.

With ARP automatic scanning enabled on an interface, the switch 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 switch 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.

NOTE:

HP recommends that you use ARP automatic scanning and fixed ARP in a small-scale network such as a cybercafé.

Configuration procedure

Follow these steps to configure ARP automatic scanning and fixed ARP:

| To do... | Use the command... | Remarks |
|----------------------|---|---------|
| Enter system view | system-view | — |
| Enter interface view | interface <i>interface-type interface-number</i> | — |

| To do... | Use the command... | Remarks |
|-------------------------------|---|----------|
| Enable ARP automatic scanning | arp scan [<i>start-ip-address to end-ip-address</i>] | Required |
| Return to system view | quit | — |
| Enable fixed ARP | arp fixup | Required |

NOTE:

- IP addresses already 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 switch supports. As a result, the switch 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.

Configuring ARP gateway protection

Introduction

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 procedure

Follow these steps to configure ARP gateway protection:

| To do... | Use the command... | Remarks |
|---|---|----------------------------------|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet port view/Layer 2 aggregate interface view | interface <i>interface-type interface-number</i> | — |
| Enable ARP gateway protection for a specified gateway | arp filter source ip-address | Required Disabled by default. |

NOTE:

- 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, ARP gateway protection applies first.
-

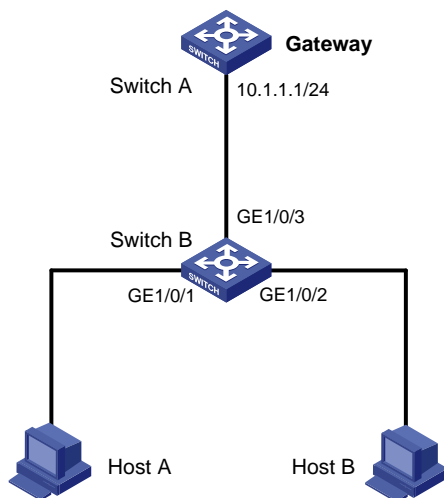
ARP gateway protection configuration example

Network requirements

As shown in Figure 87, 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 87 Network diagram for ARP gateway protection configuration



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

Introduction

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 procedure

Follow these steps to configure ARP filtering:

| To do... | Use the command... | Remarks |
|---|--|--|
| Enter system view | system-view | — |
| Enter Layer 2 Ethernet port view/Layer 2 aggregate interface view | interface <i>interface-type</i> <i>interface-number</i> | — |
| Configure an ARP filtering entry | arp filter binding <i>ip-address mac-address</i> | Required Not configured by default. |

NOTE:

- 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, ARP filtering applies first.

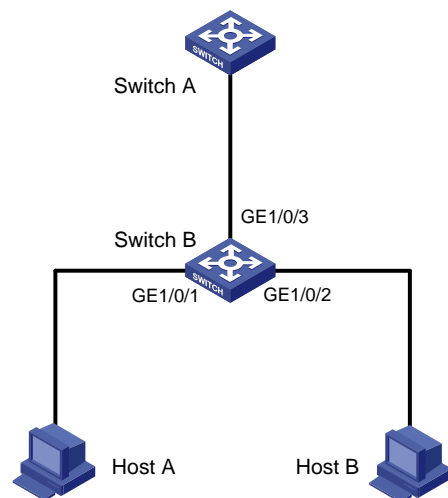
ARP filtering configuration example

Network requirements

As shown in Figure 88, the IP and MAC addresses of Host A are 10.1.1.2 and 000f-e349-1233 respectively. The IP and MAC addresses of Host B are 10.1.1.3 and 000f-e349-1234, respectively.

Configure ARP filtering on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch B to permit specific ARP packets only.

Figure 88 Network diagram for ARP filtering configuration



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 10.1.1.3 and 000f-e349-1234 and discard other ARP packets.

ND attack defense configuration

Introduction to ND attack defense

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.

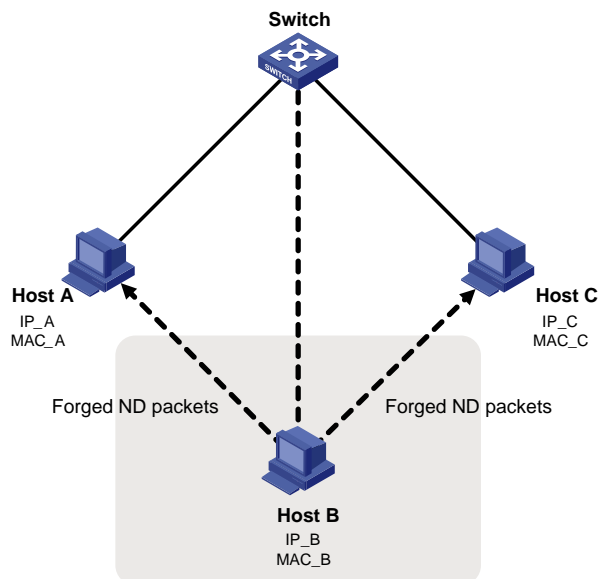
The ND protocol implements its function by using the following types of ICMPv6 messages:

- Neighbor Solicitation (NS)
- Neighbor Advertisement (NA)
- Router Solicitation (RS)
- Router Advertisement (RA)
- Redirect (RR)

An attacker can attack a network by sending forged ICMPv6 messages, as shown in [Figure 89](#):

- 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 89 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 features.

NOTE:

For more information about the functions of the ND protocol, see the *Layer 3—IP Services Configuration Guide*.

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.

Follow these steps to enable source MAC consistency check for ND packets:

| To do... | Use the command... | Remarks |
|--|---------------------------------|----------------------------------|
| Enter system view | system-view | — |
| Enable source MAC consistency check for ND packets | ipv6 nd mac-check enable | Required 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 bindings 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.

NOTE:

- To create IPv6 static bindings with IP source guard, use the **user-bind ipv6** command. For more information, see the chapter “IP source guard configuration.”
 - The DHCPv6 snooping table is created automatically by the DHCPv6 snooping module. For more information, see the *Layer 3—IP Services Configuration Guide*.
 - The ND snooping table is created automatically by the ND snooping module. For more information, see the *Layer 3—IP Services Configuration Guide*.
-

Configuring ND detection

Follow these steps to configure ND detection:

| To do... | Use the command... | Remarks |
|--|---|---|
| Enter system view | system-view | — |
| Enter VLAN view | vlan <i>vlan-id</i> | — |
| Enable ND Detection | ipv6 nd detection enable | Required Disabled by default. |
| Quit system view | quit | — |
| Enter Layer 2 Ethernet interface view or Layer 2 aggregate interface view | interface <i>interface-type interface-number</i> | — |
| Configure the port as an ND-trusted port | ipv6 nd detection trust | Optional A port does not trust sources of ND packets by default. |

NOTE:

- 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, ensure 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.
-

Displaying and maintaining ND detection

| To do... | Use the command | Remarks |
|--|--|------------------------|
| Display the ND detection configuration | display ipv6 nd detection [[{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Display the statistics of discarded packets when the ND detection checks the user legality | display ipv6 nd detection statistics [interface <i>interface-type interface-number</i>] [[{ begin exclude include } <i>regular-expression</i>] | Available in any view |
| Clear the statistics by ND detection | reset ipv6 nd detection statistics [interface <i>interface-type interface-number</i>] | Available in user view |

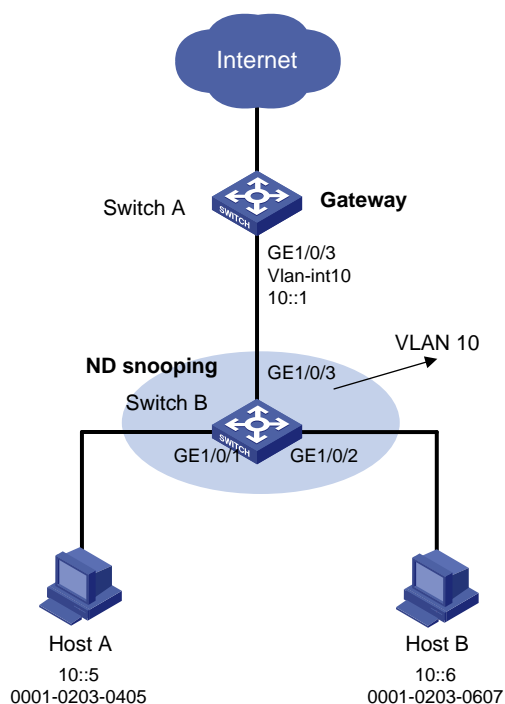
ND detection configuration example

Network requirements

As shown in [Figure 90](#), 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 90 Network diagram for ND detection configuration



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
```

Assign ports GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3 to VLAN 10.

```
[SwitchB] interface GigabitEthernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
```

```
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 10
```

```
[SwitchB-GigabitEthernet1/0/1] quit
```

```
[SwitchB] interface GigabitEthernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
```

```
[SwitchB-GigabitEthernet1/0/2] port trunk permit 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 in VLAN 10.

```
[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-GigabitEthernet 1/0/3] 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.

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 A-Series 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>

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. |
| <i>Italic</i> | <i>Italic</i> 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.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [K](#) [L](#) [M](#) [N](#) [P](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#)

A

A comparison of EAP relay and EAP termination, [67](#)
AAA for 802.1X users by a RADIUS server, [50](#)
AAA for Telnet users by an HWTACACS server, [44](#)
AAA for Telnet users by separate servers, [45](#)
Access control methods, [71](#)
Access device as the initiator, [66](#)
ACL assignment, [97](#)
ACL assignment configuration example, [105](#)
Adding a web proxy server port number, [120](#)
ARP detection configuration example I, [273](#)
ARP detection configuration example II, [275](#)
ARP filtering configuration example, [281](#)
ARP gateway protection configuration example, [280](#)
ARP restricted forwarding configuration example, [276](#)
Asymmetric key algorithm applications, [179](#)
Authentication approaches, [96](#)
Authentication/Authorization for SSH/Telnet users by a RADIUS server, [47](#)

B

Basic concepts, [179](#)

C

Cannot change port security mode when a user is online, [160](#)
Cannot configure secure MAC addresses, [160](#)
Cannot set the port security mode, [159](#)
Configuration prerequisites, [231](#)
Configuration prerequisites, [100](#)
Configuration prerequisites, [98](#)
Configuration prerequisites, [245](#)
Configuration prerequisites, [242](#)
Configuration prerequisites, [74](#)
Configuration prerequisites, [91](#)
Configuration prerequisites, [148](#)
Configuration prerequisites, [145](#)
Configuration prerequisites, [144](#)
Configuration prerequisites, [36](#)

Configuration prerequisites, [161](#)
Configuration procedure, [270](#)
Configuration procedure, [91](#)
Configuration procedure, [148](#)
Configuration procedure, [245](#)
Configuration procedure, [281](#)
Configuration procedure, [279](#)
Configuration procedure, [278](#)
Configuration procedure, [243](#)
Configuration procedure, [144](#)
Configuration procedure, [98](#)
Configuration procedure, [145](#)
Configuration procedure, [269](#)
Configuration procedure, [100](#)
Configuration procedure, [177](#)
Configuration procedure, [268](#)
Configuring a certificate attribute-based access control policy, [204](#)
Configuring a client public key, [212](#)
Configuring a peer public key manually, [182](#)
Configuring a portal-free rule, [119](#)
Configuring a RADIUS user, [42](#)
Configuring a static IPv4 source guard binding entry, [252](#)
Configuring a static IPv6 source guard binding entry, [253](#)
Configuring AAA accounting methods for an ISP domain, [40](#)
Configuring AAA authentication methods for an ISP domain, [37](#)
Configuring AAA authorization methods for an ISP domain, [39](#)
Configuring an 802.1X guest VLAN, [82](#)
Configuring an Auth-Fail VLAN, [83](#)
Configuring an HABP client, [175](#)
Configuring an SSH user, [213](#)
Configuring ARP detection based on specified objects, [272](#)
Configuring ARP packet rate limit, [267](#)

- Configuring ARP restricted forwarding, [273](#)
- Configuring ARP source suppression, [266](#)
- Configuring HWTACACS schemes, [30](#)
- Configuring intrusion protection, [147](#)
- Configuring ISP domain attributes, [36](#)
- Configuring Layer 2 portal authentication, [124](#)
- Configuring local users, [16](#)
- Configuring ND detection, [285](#)
- Configuring NTK, [146](#)
- Configuring port security traps, [147](#)
- Configuring RADIUS schemes, [20](#)
- Configuring the authentication trigger function, [79](#)
- Configuring the autoLearn mode, [150](#)
- Configuring the dynamic IPv4 source guard binding function, [252](#)
- Configuring the dynamic IPv6 source guard binding function, [254](#)
- Configuring the HABP server, [175](#)
- Configuring the local portal server, [117](#)
- Configuring the macAddressElseUserLoginSecure mode, [156](#)
- Configuring the online user handshake function, [78](#)
- Configuring the SFTP connection idle timeout period, [231](#)
- Configuring the user interfaces for SSH clients, [212](#)
- Configuring the userLoginWithOUI mode, [152](#)
- Configuring whether first-time authentication is supported, [216](#)
- Creating a user profile, [161](#)
- Creating an asymmetric key pair, [180](#)
- Creating an ISP domain, [36](#)
- Customizing authentication pages, [114](#)

D

- Destroying an asymmetric key pair, [181](#)
- Displaying and maintaining ARP defense against IP packet attacks, [267](#)
- Displaying and maintaining ARP detection, [273](#)
- Displaying and maintaining ND detection, [285](#)
- Displaying and maintaining source MAC address based ARP attack detection, [269](#)
- Displaying help information, [234](#)
- Displaying or exporting the local RSA or DSA host public key, [180](#)
- Domain-based user management, [9](#)

- Dynamic IPv4 source guard binding by DHCP relay configuration example, [260](#)
- Dynamic IPv4 source guard binding by DHCP snooping configuration example, [259](#)
- Dynamic IPv6 source guard binding by DHCPv6 snooping configuration example, [262](#)
- Dynamic IPv6 source guard binding by ND snooping configuration example, [263](#)

E

- EAD fast deployment implementation, [91](#)
- EAP over RADIUS, [66](#)
- EAP relay, [68](#)
- EAP termination, [69](#)
- Enabling 802.1X, [75](#)
- Enabling ARP black hole routing, [267](#)
- Enabling ARP detection based on static IP source guard binding Entries/DHCP snooping entries/802.1X security entries/OUI MAC addresses, [271](#)
- Enabling password control, [167](#)
- Enabling support for portal user moving, [121](#)
- Enabling the periodic online user re-authentication function, [81](#)
- Enabling the quiet timer, [81](#)
- Enabling the SFTP server, [231](#)
- Enabling the SSH server function, [211](#)
- Establishing a connection between the SSH client and server, [217](#)
- Establishing a connection to the SFTP server, [232](#)
- Extended portal functions, [108](#)

F

- Failed to request a local certificate, [206](#)
- Failed to retrieve a CA certificate, [206](#)
- Failed to retrieve CRLs, [207](#)

G

- Generating a DSA or RSA key pair, [211](#)
- Global static binding excluded port configuration example, [257](#)
- Guest VLAN, [97](#)

H

- How does PKI work, [189](#)
- How does SSH work, [208](#)
- HWTACACS, [7](#)

I

- Importing a peer public key from a public key file, [184](#)
- Inconsistent keys on the access device and the portal server, [128](#)
- Incorrect server port number on the access device, [128](#)
- Introduction, [278](#)
- Introduction, [270](#)
- Introduction, [268](#)
- Introduction, [269](#)
- Introduction, [270](#)
- Introduction, [280](#)
- Introduction, [266](#)
- Introduction, [267](#)
- Introduction, [279](#)
- Introduction to IP source guard, [249](#)
- Introduction to ND detection, [284](#)
- Introduction to portal, [108](#)
- Introduction to SSH2.0, [208](#)
- IP source guard binding, [249](#)

K

- Key algorithm types, [179](#)

L

- Layer 2 portal authentication process, [111](#)
- Level switching authentication for Telnet users by an HWTACACS server, [56](#)
- Local MAC authentication configuration example, [101](#)

M

- MAC authentication timers, [97](#)

N

- Neither static binding entries nor the dynamic binding function can be configured, [264](#)
- Network requirements, [176](#)

P

- Packet format, [64](#)
- PKI applications, [188](#)
- PKI architecture, [188](#)
- PKI terms, [187](#)
- Port security features, [140](#)
- Port security modes, [140](#)
- Portal authentication modes, [111](#)
- Portal system components, [108](#)

- Portal system using the local portal server, [110](#)
- Protocols and standards, [11](#)

R

- RADIUS, [2](#)
- RADIUS attributes, [11](#)
- RADIUS authentication and authorization for Telnet users by a network device, [59](#)
- RADIUS server feature of the device, [10](#)
- RADIUS server functions configuration task list, [42](#)
- RADIUS-based MAC authentication configuration example, [103](#)
- Requesting a certificate from a CA running RSA Keon, [198](#)
- Requesting a certificate from a CA running Windows 2003 Server, [201](#)

S

- Setting a local user password in interactive mode, [170](#)
- Setting global password control parameters, [167](#)
- Setting local user password control parameters, [169](#)
- Setting super password control parameters, [170](#)
- Setting the 802.1X authentication timeout timers, [78](#)
- Setting the maximum number of authentication request attempts, [78](#)
- Setting the maximum number of concurrent 802.1X users on a port, [77](#)
- Setting the maximum number of online portal users, [119](#)
- Setting the port authorization state, [76](#)
- Setting the SSH management parameters, [214](#)
- Setting user group password control parameters, [168](#)
- Specifying a mandatory authentication domain on a port, [80](#)
- Specifying a RADIUS client, [43](#)
- Specifying a source IP address or interface for the SFTP client, [232](#)
- Specifying a source IP address/interface for the SSH client, [215](#)
- Specifying an access control method, [77](#)
- Specifying an authentication domain for portal users, [120](#)
- Specifying EAP relay or EAP termination, [75](#)
- Specifying the local portal server for Layer 2 portal authentication, [114](#)
- SSH client configuration task list, [215](#)
- SSH server configuration task list, [210](#)
- SSL handshake failure, [246](#)

- SSL protocol stack, [242](#)
- SSL security mechanism, [241](#)
- SSL server policy configuration example, [243](#)
- Static IPv4 source guard binding entry configuration example, [256](#)
- Static IPv6 source guard binding entry configuration example, [261](#)
- Submitting a certificate request in auto mode, [193](#)
- Submitting a certificate request in manual mode, [193](#)
- Support for guest VLAN and Auth-Fail VLAN, [143](#)

T

- Terminating the connection to the remote SFTP server, [234](#)
- Triple authentication basic function configuration example, [132](#)
- Triple authentication mechanism, [130](#)
- Triple authentication supporting VLAN assignment and Auth-Fail VLAN configuration example, [135](#)
- Troubleshooting HWTACACS, [62](#)
- Troubleshooting RADIUS, [61](#)

U

- User account policies, [96](#)
- Using 802.1X authentication with other features, [71](#)
- Using triple authentication with other features, [131](#)

V

- VLAN assignment, [97](#)

W

- Web browser users cannot be correctly redirected, [95](#)
- When switch acts as client for password authentication, [225](#)
- When switch acts as client for publickey authentication, [228](#)
- When switch acts as server for password authentication, [218](#)
- When switch acts as server for publickey authentication, [220](#)
- Working with SFTP directories, [233](#)
- Working with SFTP files, [233](#)