

HP V1910 Switch Series

User Guide



Part number: 5998-2238

Document version: 2



The HP V1910 Switch Series User Guide describes the software features for the HP 1910 switches and guides you through the software configuration procedures. It also provides configuration examples to help you apply software features to different network scenarios.

This documentation set is intended for:

- Network planners
- Field technical support and servicing engineers
- Network administrators working with the HP V1910 switches

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.

Warranty

The Hewlett-Packard Limited Warranty Statement for this product and the HP Software License Terms which apply to any software accompanying this product are available on the HP networking Web site at <http://www.hp.com/networking/warranty>. The customer warranty support and services information are available on the HP networking Web site at <http://www.hp.com/networking/support>. Additionally, your HP-authorized network reseller can provide you with assistance, both with services that they offer and with services offered by HP.

Contents

Overview	1
Configuration through the web interface	2
Web-based network management operating environment	2
Logging in to the web interface	2
Default login information	2
Example	3
Logging out of the web interface	4
Introduction to the web interface	4
Web user level	5
Introduction to the web-based NM functions	5
Introduction to the common items on the web pages	13
Configuration guidelines	15
Configuration at the CLI	16
Getting started with the CLI	16
Setting up the configuration environment	16
Setting terminal parameters	17
Logging in to the CLI	20
CLI commands	21
initialize	21
ipsetup	21
password	22
ping	23
quit	23
reboot	24
summary	24
upgrade	25
Configuration example for upgrading the system software image at the CLI	26
Configuration wizard	28
Overview	28
Basic service setup	28
Entering the configuration wizard homepage	28
Configuring system parameters	28
Configuring management IP address	29
Finishing configuration wizard	31
IRF stack management	32
Configuring stack management	32
Stack management configuration task list	32
Configuring global parameters of a stack	33
Configuring stack ports	35
Displaying topology summary of a stack	35
Displaying device summary of a stack	36
Logging into a member switch from the master switch	36
Stack configuration example	36
Configuration guidelines	42

Summary	43
Displaying device summary	43
Displaying system information	43
Displaying device information	44
Device basic information configuration	46
Configuring device basic information	46
Configuring system name	46
Configuring idle timeout period	46
System time configuration	48
Configuring system time	48
System time configuration example	49
Configuration guidelines	51
Log management configuration	52
Configuring log management	52
Configuration task list	52
Setting syslog related parameters	52
Displaying syslog	53
Setting loghost	55
Configuration management	56
Back up configuration	56
Restore configuration	56
Save configuration	57
Initialize	58
Device maintenance	59
Software upgrade	59
Device reboot	60
Electronic label	61
Diagnostic information	61
File management	63
File management configuration	63
Displaying file list	63
Downloading a file	64
Uploading a file	64
Removing a file	64
Port management configuration	65
Configuring a port	65
Setting operation parameters for a port	65
Viewing the operation parameters of a port	69
Port management configuration example	70
Port mirroring configuration	74
Introduction to port mirroring	74
Implementing port mirroring	74
Configuring local port mirroring	75
Configuration task list	75
Creating a mirroring group	75
Configuring ports for a mirroring group	76
Configuration examples	78
Local port mirroring configuration example	78
Configuration guidelines	81

User management	82
Overview	82
Managing users	82
Adding a local user	82
Setting the super password	83
Switching to the management level	84
Loopback test configuration	85
Overview	85
Loopback operation	85
Configuration guidelines	86
VCT	87
Overview	87
Testing cable status	87
Flow interval configuration	89
Overview	89
Monitoring port traffic statistics	89
Setting the traffic statistics generating interval	89
Viewing port traffic statistics	89
Storm constrain configuration	91
Overview	91
Configuring storm constrain	91
Setting the traffic statistics generating interval	91
Configuring storm constrain	92
RMON configuration	95
Working mechanism	95
RMON groups	96
Configuring RMON	97
Configuration task list	97
Configuring a statistics entry	99
Configuring a history entry	100
Configuring an event entry	101
Configuring an alarm entry	102
Displaying RMON statistics information	104
Displaying RMON history sampling information	106
Displaying RMON event logs	108
RMON configuration example	108
Energy saving configuration	113
Overview	113
Configuring energy saving on a port	113
SNMP configuration	115
SNMP mechanism	115
SNMP protocol version	116
SNMP configuration	116
Configuration task list	116
Enabling SNMP	117
Configuring an SNMP view	119
Configuring an SNMP community	121
Configuring an SNMP group	122
Configuring an SNMP user	123

Configuring SNMP trap function.....	125
SNMP configuration example	127
Interface statistics	133
Overview	133
Displaying interface statistics.....	133
VLAN configuration	135
Introduction to VLAN	135
VLAN fundamentals.....	135
VLAN types.....	136
Introduction to port-based VLAN.....	137
Configuring a VLAN.....	138
Configuration task list.....	138
Creating VLANs.....	138
Selecting VLANs.....	139
Modifying a VLAN.....	140
Modifying ports.....	142
VLAN configuration example	143
Configuration guidelines.....	148
VLAN interface configuration.....	149
Configuring VLAN interfaces.....	149
Configuration task list.....	149
Creating a VLAN interface	149
Modifying a VLAN interface.....	150
Voice VLAN configuration.....	153
OUI addresses.....	153
Voice VLAN assignment modes	153
Security mode and normal mode of voice VLANs	155
Configuring the voice VLAN.....	155
Configuration task list.....	155
Configuring voice VLAN globally.....	157
Configuring voice VLAN on a port	157
Adding OUI addresses to the OUI list.....	159
Voice VLAN configuration examples.....	160
Configuring voice VLAN on a port in automatic voice VLAN assignment mode	160
Configuring a voice VLAN on a port in manual voice VLAN assignment mode.....	165
Configuration guidelines.....	171
MAC address configuration.....	172
Configuring MAC addresses.....	173
Configuring a MAC address entry	173
Setting the aging time of MAC address entries.....	175
MAC address configuration example.....	176
MSTP configuration.....	177
STP 177	
STP protocol packets	177
Basic concepts in STP.....	177
How STP works	178
RSTP.....	184
MSTP	185
STP and RSTP limitations	185
MSTP features.....	185

MSTP basic concepts.....	185
How MSTP works.....	189
Implementation of MSTP on devices.....	189
Protocols and standards.....	190
Configuring MSTP.....	190
Configuration task list.....	190
Configuring an MST region.....	190
Configuring MSTP globally.....	192
Configuring MSTP on a port.....	194
Displaying MSTP information of a port.....	196
MSTP configuration example.....	199
Configuration guidelines.....	203
Link aggregation and LACP configuration.....	205
Basic concepts.....	205
Link aggregation modes.....	206
Load sharing mode of an aggregation group.....	208
Configuring link aggregation and LACP.....	208
Configuration task list.....	208
Creating a link aggregation group.....	209
Displaying information of an aggregate interface.....	211
Setting LACP priority.....	211
Displaying information of LACP-enabled ports.....	212
Link aggregation and LACP configuration example.....	214
Configuration guidelines.....	217
LLDP configuration.....	218
Background.....	218
Basic concepts.....	218
How LLDP works.....	222
Compatibility of LLDP with CDP.....	222
Protocols and standards.....	223
Configuring LLDP.....	223
LLDP configuration task list.....	223
Enabling LLDP on ports.....	224
Configuring LLDP settings on ports.....	225
Configuring global LLDP setup.....	229
Displaying LLDP information for a port.....	231
Displaying global LLDP information.....	236
Displaying LLDP information received from LLDP neighbors.....	238
LLDP configuration examples.....	238
Basic LLDP configuration example.....	238
CDP-compatible LLDP configuration example.....	244
Configuration guidelines.....	250
IGMP snooping configuration.....	251
Overview.....	251
Principle of IGMP snooping.....	251
IGMP snooping related ports.....	251
Work mechanism of IGMP snooping.....	252
IGMP snooping querier.....	254
Protocols and standards.....	254
Configuring IGMP snooping.....	254
Configuration task list.....	254

Enabling IGMP snooping globally.....	255
Configuring IGMP snooping in a VLAN	256
Configuring IGMP snooping port functions	257
Display IGMP snooping multicast entry information	258
IGMP snooping configuration example.....	259
Routing configuration.....	266
Routing table	266
Static route.....	266
Default route	267
Configuring IPv4 routing.....	267
Displaying the IPv4 active route table	267
Creating an IPv4 static route	268
Static route configuration example	269
Precautions	273
DHCP overview.....	274
Introduction to DHCP.....	274
DHCP address allocation.....	274
Allocation mechanisms.....	274
Dynamic IP address allocation process	275
IP address lease extension	275
DHCP message format	276
DHCP options.....	277
DHCP options overview	277
Introduction to DHCP options	277
Introduction to Option 82	277
Protocols and standards.....	278
DHCP relay agent configuration.....	279
Introduction to DHCP relay agent	279
Application environment	279
Fundamentals	279
DHCP relay agent configuration task list.....	280
Enabling DHCP and configuring advanced parameters for the DHCP relay agent.....	281
Creating a DHCP server group	282
Enabling the DHCP relay agent on an interface	283
Configuring and displaying clients' IP-to-MAC bindings.....	284
DHCP relay agent configuration example	285
DHCP snooping configuration	288
DHCP snooping overview	288
Functions of DHCP snooping	288
Application environment of trusted ports.....	289
DHCP snooping support for Option 82	290
DHCP snooping configuration task list	290
Enabling DHCP snooping	291
Configuring DHCP snooping functions on an interface.....	293
Displaying clients' IP-to-MAC bindings.....	293
DHCP snooping configuration example.....	294
Service management configuration	299
Configuring service management	300
Diagnostic tools.....	302
Ping	302

Trace route.....	302
Diagnostic tool operations.....	303
Ping operation.....	303
Trace route operation.....	304
ARP management.....	306
ARP overview.....	306
ARP function.....	306
ARP message format.....	306
ARP operation.....	307
ARP table.....	307
Managing ARP entries.....	308
Displaying ARP entries.....	308
Creating a static ARP entry.....	309
Static ARP configuration example.....	309
Gratuitous ARP.....	313
Introduction to gratuitous ARP.....	313
Configuring gratuitous ARP.....	313
ARP attack defense configuration.....	315
ARP detection.....	315
Introduction to ARP detection.....	315
Configuring ARP detection.....	317
Creating a static binding entry.....	319
802.1X fundamentals.....	320
Architecture of 802.1X.....	320
Controlled/uncontrolled port and port authorization status.....	320
802.1X-related protocols.....	321
Packet formats.....	321
EAP over RADIUS.....	323
Initiating 802.1X authentication.....	323
802.1X client as the initiator.....	323
Access device as the initiator.....	323
802.1X authentication procedures.....	324
A comparison of EAP relay and EAP termination.....	324
EAP relay.....	325
EAP termination.....	327
802.1X configuration.....	328
HP implementation of 802.1X.....	328
Access control methods.....	328
Using 802.1X authentication with other features.....	328
Configuring 802.1X.....	329
Configuration prerequisites.....	329
802.1X configuration task list.....	330
Configuring 802.1X globally.....	330
Configuring 802.1X on a port.....	332
Configuration examples.....	334
802.1X configuration example.....	334
ACL assignment configuration example.....	341
AAA configuration.....	351
Overview.....	351
Introduction to AAA.....	351

Domain-based user management.....	352
Configuring AAA.....	352
Configuration prerequisites.....	352
Configuration task list.....	352
Configuring an ISP domain.....	353
Configuring authentication methods for the ISP domain.....	354
Configuring authorization methods for the ISP domain.....	355
Configuring accounting methods for the ISP domain.....	356
AAA configuration example.....	358
RADIUS configuration.....	363
Introduction to RADIUS.....	363
Client/server model.....	363
Security and authentication mechanisms.....	363
Basic message exchange process of RADIUS.....	364
RADIUS packet format.....	365
Extended RADIUS attributes.....	367
Protocols and standards.....	368
Configuring RADIUS.....	368
Configuration task list.....	368
Configuring RADIUS servers.....	369
Configuring RADIUS parameters.....	370
RADIUS configuration example.....	373
Configuration guidelines.....	378
Users.....	379
Configuring users.....	379
Configuring a local user.....	379
Configuring a user group.....	381
PKI configuration.....	383
PKI overview.....	383
PKI terms.....	383
Architecture of PKI.....	383
Applications of PKI.....	384
Operation of PKI.....	385
Configuring PKI.....	385
Configuration task list.....	385
Creating a PKI entity.....	388
Creating a PKI domain.....	389
Generating an RSA key pair.....	392
Destroying the RSA key pair.....	392
Retrieving a certificate.....	393
Requesting a local certificate.....	395
Retrieving and displaying a CRL.....	396
PKI configuration example.....	397
Configuring a PKI entity to request a certificate from a CA.....	397
Configuration guidelines.....	402
Port isolation group configuration.....	403
Overview.....	403
Configuring a port isolation group.....	403
Port isolation group configuration example.....	404

Authorized IP configuration.....	406
Overview	406
Configuring authorized IP.....	406
Authorized IP configuration example	407
Authorized IP configuration example	407
ACL configuration	410
ACL overview	410
Introduction to IPv4 ACL.....	410
Effective period of an ACL.....	411
ACL step.....	412
Configuring an ACL.....	412
Configuration task list.....	412
Configuring a time range	413
Creating an IPv4 ACL.....	414
Configuring a rule for a basic IPv4 ACL	414
Configuring a rule for an advanced IPv4 ACL	416
Configuring a rule for an Ethernet frame header ACL.....	419
Configuration guidelines.....	421
QoS configuration.....	422
Introduction to QoS	422
Networks without QoS guarantee	422
QoS requirements of new applications.....	422
Congestion: causes, impacts, and countermeasures	422
End-to-end QoS.....	424
Traffic classification	424
Packet precedences.....	425
Queue scheduling.....	427
Line rate	429
Priority mapping	430
Introduction to priority mapping tables	431
QoS configuration	432
Configuration task lists	432
Creating a class.....	434
Configuring match criteria	435
Creating a traffic behavior	437
Configuring traffic mirroring and traffic redirecting for a traffic behavior.....	438
Configuring other actions for a traffic behavior.....	439
Creating a policy.....	440
Configuring classifier-behavior associations for the policy.....	440
Applying a policy to a port	441
Configuring queue scheduling on a port	442
Configuring line rate on a port	443
Configuring priority mapping tables	444
Configuring priority trust mode on a port	445
Configuration guidelines.....	447
ACL/QoS configuration examples	448
ACL/QoS configuration example.....	448
PoE configuration	458
PoE overview	458
Advantages	458
Composition	458

Protocol specification	459
Configuring PoE	459
Configuring PoE ports	459
Configuring non-standard PD detection	461
Displaying information about PSE and PoE ports	462
PoE configuration example	462
Support and other resources	465
Contacting HP	465
Related information	465
Conventions	465
Subscription service	466
Index	467

Overview

The HP V1910 Switch Series can be configured through the command line interface (CLI), web interface, and SNMP/MIB. These configuration methods are suitable for different application scenarios.

- The web interface supports all V1910 Switch Series configurations.
- The CLI provides some configuration commands to facilitate your operation. To perform other configurations not supported by the CLI, use the web interface.

Configuration through the web interface

Web-based network management operating environment

HP provides the web-based network management function to facilitate the operations and maintenance on HP's network devices. Through this function, the administrator can visually manage and maintain network devices through the web-based configuration interfaces.

a. Web-based network management operating environment



Logging in to the web interface

Default login information

The device is provided with the default Web login information. You can use the default information to log in to the web interface.

1. The default web login information

Information needed at login	Default value
Username	admin
Password	None
IP address of the device (VLAN-interface 1)	Default IP address of the device, depending on the status of the network where the device resides.

Table 1 The device is not connected to the network, or no DHCP server exists in the subnet where the device resides

If the device is not connected to the network, or no DHCP server exists in the subnet where the device resides, you can get the default IP address of the device on the label on the device, as shown in **b**. The default subnet mask is 255.255.0.0.

b. Default IP address of the device

Default IP Address: 169.254.52.86

Table 2 A DHCP server exists in the subnet where the device resides

If a DHCP server exists in the subnet where the device resides, the device will dynamically obtain its default IP address through the DHCP server. You can log in to the device through the console port, and execute the **summary** command to view the information of its default IP address.

```
<Sysname> summary
Select menu option:          Summary
IP Method:                   DHCP
IP address:                   10.153.96.86
Subnet mask:                  255.255.255.0
Default gateway:              0.0.0.0
<Omitted>
```

Example

Assuming that the default IP address of the device is 169.254.52.86, follow these steps to log in to the device through the web interface.

- Connect the device to a PC

Connect the GigabitEthernet interface of the device to a PC by using a crossover Ethernet cable (by default, all interfaces belong to VLAN 1).

- Configure an IP address for the PC and ensure that the PC and device can communicate with each other properly.

Select an IP address for the PC from network segment 169.254.0.0/16 (except for the default IP address of the device), for example, 169.254.52.86.

- Open the browser, and input the login information.

On the PC, open the browser (IE 5.0 or later), type the IP address `http://169.254.52.86` in the address bar, and press **Enter** to enter the login page of the web interface, as shown in **a**. Input the username **admin** and verification code, leave the password blank, and click **Login**.

a. Login page of the web interface



The screenshot shows a web interface for logging in. It has a title "Web User Login" and three input fields: "User Name", "Password", and "Verify Code". The "Verify Code" field contains the text "C68Z". Below the input fields is a "Login" button.

CAUTION:

- The PC where you configure the device is not necessarily a web-based network management terminal. A web-based network management terminal is a PC used to log in to the web interface and is required to be reachable to the device.
- After logging in to the web interface, you can select **Device** → **Users** from the navigation tree, create a new user, and select **Wizard** or **Network** → **VLAN interface** to configure the IP address of the VLAN interface acting as the management interface. For more information, see the corresponding configuration guides of these modules.
- If you click the verification code displayed on the web login page, you can get a new verification code.
- Up to five users can concurrently log in to the device through the web interface.

Logging out of the web interface

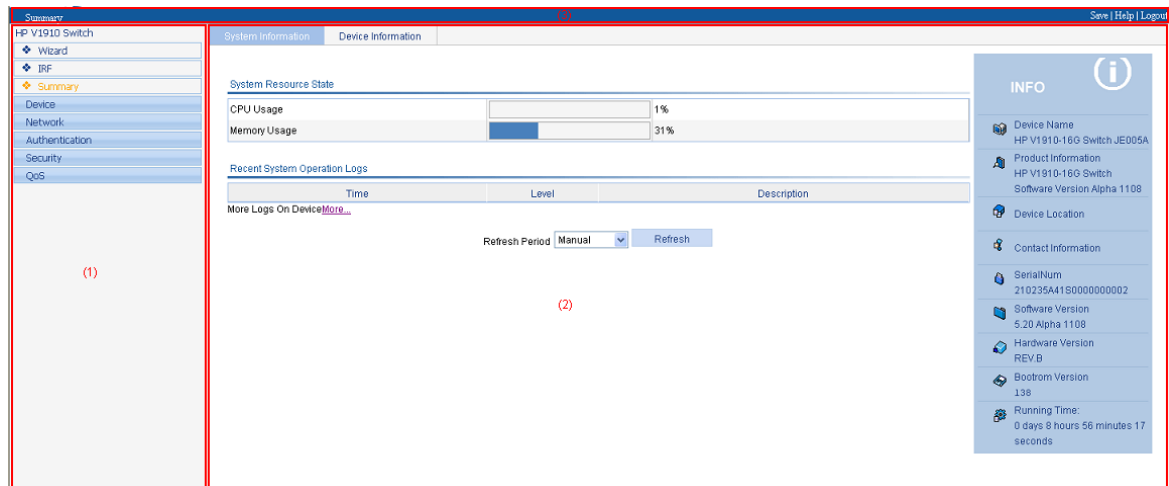
Click **Logout** in the upper-right corner of the web interface, as shown in a to quit the web console.

The system does not save the current configuration automatically. Therefore, it is recommended to save the current configuration before logout.

Introduction to the web interface

The Web interface is composed of three parts: navigation tree, title area, and body area, as shown in a.

a. Web-based configuration interface



(1) Navigation tree

(2) Body area

(3) Title area

- Navigation tree—Organizes the web-based NM functions as a navigation tree, where you can select and configure functions as needed. The result is displayed in the body area.
- Body area—Allows you to configure and display features.
- Title area—Displays the path of the current configuration interface in the navigation tree; provides the **Help** button to display the web related help information, and the **Logout** button to log out of the web interface.

CAUTION:

The web network management functions not supported by the device are not displayed in the navigation tree.

Web user level

Web user levels, from low to high, are **visitor**, **monitor**, **configure**, and **management**. A user with a higher level has all the operating rights of a user with a lower level.

- Visitor—Users of this level can only use the network diagnostic tools **ping** and **Trace Route**. They can neither access the device data nor configure the device.
- Monitor—Users of this level can only access the device data but cannot configure the device.
- Configure—Users of this level can access device data and configure the device, but they cannot upgrade the host software, add/delete/modify users, or back up/restore configuration files.
- Management—Users of this level can perform any operations to the device.

Introduction to the web-based NM functions

NOTE:

User level in 1 indicates that users of this level or users of a higher level can perform the corresponding operations.

1. Description of Web-based NM functions

Function menu		Description	User level
Wizard	IP Setup	Allows you to perform quick configuration of the device.	Management
	Setup	Displays global settings and port settings of a stack.	Configure
IRF		Allows you to configure global parameters and stack ports.	Management
Summary	Topology Summary	Displays the topology summary of a stack.	Configure
	Device Summary	Displays the control panels of stack members.	Configure
	System Information	Displays the basic system information, system resource state, and recent system operation logs.	Monitor
Device	Device Information	Displays the port information of the device.	Monitor
	Basic	System Name	Displays and allows you to configure the system name.
Web Idle Timeout		Displays and allows you to configure the idle timeout period for logged-in users.	Configure

Function menu		Description	User level
Device Maintenance	Software Upgrade	Allows you to configure to upload upgrade file from local host, and upgrade the system software.	Management
	Reboot	Allows you to configure to reboot the device.	Management
	Electronic Label	Displays the electronic label of the device.	Monitor
	Diagnostic Information	Generates diagnostic information file, and allows you to view or save the file to local host.	Management
System Time	System Time	Displays and allows you to configure the system date and time.	Configure
Syslog	Loglist	Displays and refreshes system logs. Allows you to clear system logs.	Monitor Configure
	Loghost	Displays and allows you to configure the loghost.	Configure
	Log Setup	Displays and allows you to configure the buffer capacity, and interval for refreshing system logs.	Configure
	Backup	Allows you to back up the configuration file to be used at the next startup from the device to the host of the current user.	Management
Configuration	Restore	Allows you to upload the configuration file to be used at the next startup from the host of the current user to the device.	Management
	Save	Allows you to save the current configuration to the configuration file to be used at the next startup.	Configure
	Initialize	Allows you to restore the factory default settings.	Configure
File Management	File Management	Allows you to manage files on the device, such as displaying the file list, downloading a file, uploading a file, and removing a file.	Management
Port Management	Summary	Displays port information by features.	Monitor
	Detail	Displays feature information by ports.	Monitor
	Setup	Allows you to create, modify, delete, and enable/disable a port, and clear port statistics.	Configure
Port Mirroring	Summary	Displays the configuration information of a port mirroring group.	Monitor
	Create	Allows you to create a port mirroring group.	Configure
	Remove	Allows you to remove a port mirroring group.	Configure
	Modify Port	Allows you to configure ports for a mirroring group.	Configure
Users	Summary	Displays the brief information of FTP and Telnet users.	Monitor
	Super Password	Allows you to configure a password for a lower-level user to switch from the current access level to the management level.	Management
	Create	Allows you to create an FTP or Telnet user.	Management

Function menu		Description	User level
	Modify	Allows you to modify FTP or Telnet user information.	Management
	Remove	Allows you to remove an FTP or a Telnet user.	Management
	Switch To Management	Allows you to switch the current user level to the management level.	Visitor
Loopback	Loopback	Allows you to perform loopback tests on Ethernet interfaces.	Configure
VCT	VCT	Allows you to check the status of the cables connected to Ethernet ports.	Configure
Flow Interval	Port Traffic Statistics	Displays the average rate at which the interface receives and sends packets within a specified time interval.	Monitor
	Interval Configuration	Allows you to set an interval for collecting traffic statistics on interfaces.	Configure
Storm Constrain	Storm Constrain	Displays and allows you to set the interval for collecting storm constrain statistics. Displays, and allows you to create, modify, and remove the port traffic threshold.	Configure
RMON	Statistics	Displays, and allows you to create, modify, and clear RMON statistics.	Configure
	History	Displays, and allows you to create, modify, and clear RMON history sampling information.	Configure
	Alarm	Allows you to view, create, modify, and clear alarm entries.	Configure
	Event	Allows you to view, create, modify, and clear event entries.	Configure
	Log	Displays log information about RMON events.	Configure
Energy Saving	Energy Saving	Displays and allows you to configure the energy saving settings of an interface.	Configure
SNMP	Setup	Displays and refreshes SNMP configuration and statistics information.	Monitor
		Allows you to configure SNMP.	Configure
	Community	Displays SNMP community information.	Monitor
		Allows you to create, modify and delete an SNMP community.	Configure
	Group	Displays SNMP group information.	Monitor
		Allows you to create, modify and delete an SNMP group.	Configure
	User	Displays SNMP user information.	Monitor
Allows you to create, modify and delete an SNMP user.		Configure	

Function menu		Description	User level
	Trap	Displays the status of the SNMP trap function and information about target hosts.	Monitor
		Allows you to enable or disable the SNMP trap function, or create, modify and delete a target host.	Configure
	View	Displays SNMP view information.	Monitor
		Allows you to create, modify and delete an SNMP view.	Configure
Interface Statistics	Interface Statistics	Displays and allows you to clear the statistics information of an interface.	Configure
VLAN	Select VLAN	Allows you to select a VLAN range.	Monitor
	Create	Allows you to create VLANs.	Configure
	Port Detail	Displays the VLAN-related details of a port.	Monitor
	Detail	Displays the member port information of a VLAN.	Monitor
	Modify VLAN	Allows you to modify the description and member ports of a VLAN.	Configure
	Modify Port	Allows you to change the VLAN to which a port belongs.	Configure
	Remove	Allows you to remove VLANs.	Configure
VLAN Interface	Summary	Displays information about VLAN interfaces by address type.	Monitor
	Create	Allows you to create VLAN interfaces and configure IP addresses for them.	Configure
	Modify	Allows you to modify the IP addresses and status of VLAN interfaces.	Configure
Voice VLAN	Remove	Allows you to remove VLAN interfaces.	Configure
	Summary	Displays voice VLAN information globally or on a port.	Monitor
	Setup	Allows you to configure the global voice VLAN.	Configure
	Port Setup	Allows you to configure a voice VLAN on a port.	Configure
	OUI Summary	Displays the addresses of the OUIs that can be identified by voice VLAN.	Monitor
	OUI Add	Allows you to add the address of an OUI that can be identified by voice VLAN.	Configure
	OUI Remove	Allows you to remove the address of an OUI that can be identified by voice VLAN.	Configure
MAC	MAC	Displays MAC address information.	Monitor
	Setup	Allows you to create and remove MAC addresses.	Configure
MSTP	Setup	Displays and allows you to configure MAC address aging time.	Configure
	Region	Displays information about MST regions.	Monitor

Function menu	Description	User level		
	Allows you to modify MST regions.	Configure		
	Global	Allows you to set global MSTP parameters.	Configure	
	Port Summary	Displays the MSTP information of ports.	Monitor	
	Port Setup	Allows you to set MSTP parameters on ports.	Configure	
Link Aggregation	Summary	Displays information about link aggregation groups.	Monitor	
	Create	Allows you to create link aggregation groups.	Configure	
	Modify	Allows you to modify link aggregation groups.	Configure	
	Remove	Allows you to remove link aggregation groups.	Configure	
LACP	Summary	Displays information about LACP-enabled ports and their partner ports.	Monitor	
	Setup	Allows you to set LACP priorities.	Configure	
LLDP	Port Setup	Displays the LLDP configuration information, local information, neighbor information, statistics information, and status information of a port.	Monitor	
		Allows you to modify LLDP configuration on a port.	Configure	
	Global Setup		Displays global LLDP configuration information.	Monitor
			Allows you to configure global LLDP parameters.	Configure
	Global Summary	Displays global LLDP local information and statistics.	Monitor	
	Neighbor Summary	Displays global LLDP neighbor information.	Monitor	
IGMP Snooping	Basic	Displays global IGMP snooping configuration information or the IGMP snooping configuration information in a VLAN, and allows you to view the IGMP snooping multicast entry information.	Monitor	
		Allows you to configure IGMP snooping globally or in a VLAN.	Configure	
	Advanced	Displays the IGMP snooping configuration information on a port.	Monitor	
		Allows you to configure IGMP snooping on a port.	Configure	
IPv4 Routing	Summary	Displays the IPv4 active route table.	Monitor	
	Create	Allows you to create an IPv4 static route.	Configure	
	Remove	Allows you to delete the selected IPv4 static routes.	Configure	
DHCP	DHCP Relay	Displays information about the DHCP status, advanced configuration information of the DHCP relay agent, DHCP server group configuration, DHCP relay agent interface configuration, and the DHCP client information.	Monitor	

Function menu		Description	User level
		Allows you to enable/disable DHCP, configure advanced DHCP relay agent settings, configure a DHCP server group, and enable/disable the DHCP relay agent on an interface.	Configure
	DHCP Snooping	Displays the status, trusted and untrusted ports and DHCP client information of DHCP snooping.	Monitor
		Allows you to enable/disable DHCP snooping, and configure DHCP snooping trusted and untrusted ports.	Configure
Service	Service	Displays the states of services: enabled or disabled.	Configure
		Allows you to enable/disable services, and set related parameters.	Management
Diagnostic Tools	Ping	Allows you to ping an IPv4 address.	Visitor
	Trace Route	Allows you to perform trace route operations.	Visitor
ARP Management	ARP Table	Displays ARP table information.	Monitor
		Allows you to add, modify, and remove ARP entries.	Configure
	Gratuitous ARP	Displays the configuration information of gratuitous ARP.	Monitor
ARP Anti-Attack	ARP Detection	Allows you to configure gratuitous ARP.	Configure
		Displays ARP detection configuration information.	Monitor
802.1X	802.1X	Allows you to configure ARP detection.	Configure
		Displays 802.1X configuration information globally or on a port.	Monitor
Authentic ation AAA	Domain Setup	Allows you to configure 802.1X globally or on a port.	Configure
		Displays ISP domain configuration information.	Monitor
	Authentication	Allows you to add and remove ISP domains.	Management
		Displays the authentication configuration information of an ISP domain.	Monitor
	Authorization	Allows you to specify authentication methods for an ISP domain.	Management
		Displays the authorization method configuration information of an ISP domain.	Monitor
Accounting	Allows you to specify authorization methods for an ISP domain.	Management	
		Displays the accounting method configuration information of an ISP domain.	Monitor








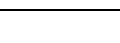
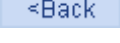

Function menu		Description	User level	
		Allows you to specify accounting methods for an ISP domain.	Management	
RADIUS	RADIUS Server	Displays and allows you to configure RADIUS server information.	Management	
	RADIUS Setup	Displays and allows you to configure RADIUS parameters.	Management	
Users	Local User	Displays configuration information about local users.	Monitor	
		Allows you to create, modify and remove a local user.	Management	
	User Group	Displays configuration information about user groups.	Monitor	
		Allows you to create, modify and remove a user group.	Management	
PKI	Entity	Displays information about PKI entities.	Monitor	
		Allows you to add, modify, and delete a PKI entity.	Configure	
	Domain	Displays information about PKI domains.	Monitor	
		Allows you to add, modify, and delete a PKI domain.	Configure	
	Certificate	Displays the certificate information of PKI domains and allows you to view the contents of a certificate.	Monitor	
		Allows you to generate a key pair, destroy a key pair, retrieve a certificate, request a certificate, and delete a certificate.	Configure	
CRL	Displays the contents of the CRL.	Monitor		
	Allows you to receive the CRL of a domain.	Configure		
Security	Port Isolate Group	Summary	Displays port isolation group information.	Monitor
		Modify	Allows you to configure a port isolation group.	Configure
	Authorized IP	Summary	Displays the configurations of authorized IP, the associated IPv4 ACL list, and the associated IPv6 ACL list.	Management
		Setup	Allows you to configure authorized IP.	Management
QoS	Time Range	Summary	Displays time range configuration information.	Monitor
		Create	Allows you to create a time range.	Configure
		Remove	Allows you to delete a time range.	Configure
	ACL IPv4	Summary	Displays IPv4 ACL configuration information.	Monitor
		Create	Allows you to create an IPv4 ACL.	Configure
		Basic Setup	Allows you to configure a rule for a basic IPv4 ACL.	Configure
		Advanced Setup	Allows you to configure a rule for an advanced IPv4 ACL.	Configure

Function menu		Description	User level	
	Link Setup	Allows you to create a rule for a link layer ACL.	Configure	
	Remove	Allows you to delete an IPv4 ACL or its rules.	Configure	
Queue	Summary	Displays the queue information of a port.	Monitor	
	Setup	Allows you to configure a queue on a port.	Configure	
Line Rate	Summary	Displays line rate configuration information.	Monitor	
	Setup	Allows you to configure the line rate.	Configure	
Classifier	Summary	Displays classifier configuration information.	Monitor	
	Create	Allows you to create a class.	Configure	
	Setup	Allows you to configure the classification rules for a class.	Configure	
	Remove	Allows you to delete a class or its classification rules.	Configure	
Behavior	Summary	Displays traffic behavior configuration information.	Monitor	
	Create	Allows you to create a traffic behavior.	Configure	
	Setup	Allows you to configure actions for a traffic behavior.	Configure	
	Port Setup	Allows you to configure traffic mirroring and traffic redirecting for a traffic behavior	Configure	
	Remove	Allows you to delete a traffic behavior.	Configure	
QoS Policy	Summary	Displays QoS policy configuration information.	Monitor	
	Create	Allows you to create a QoS policy.	Configure	
	Setup	Allows you to configure the classifier-behavior associations for a QoS policy.	Configure	
	Remove	Allows you to delete a QoS policy or its classifier-behavior associations.	Configure	
Port Policy	Summary	Displays the QoS policy applied to a port.	Monitor	
	Setup	Allows you to apply a QoS policy to a port.	Configure	
	Remove	Allows you to remove the QoS policy from the port.	Configure	
Priority Mapping	Priority Mapping	Displays priority mapping table information.	Monitor	
	Priority Mapping	Allows you to modify the priority mapping entries.	Configure	
Port Priority	Port Priority	Displays port priority and trust mode information.	Monitor	
	Port Priority	Allows you to modify port priority and trust mode.	Configure	
PoE	PoE	Summary	Displays PSE information and PoE interface information.	Monitor
	PoE	Setup	Allows you to configure a PoE interface.	Configure

Introduction to the common items on the web pages

Buttons and icons

1. Commonly used buttons and icons

Button and icon	Function
	Used to apply the configuration on the current page.
	Used to cancel the configuration on the current page, and return to the corresponding list page or the Device Info page.
	Used to refresh the information on the current page.
	Used to clear all the information on a list or all statistics.
	Used to enter a page for adding an item.
 	Used to remove the selected items.
	Used to select all the entries on a list, or all the ports on the device panel.
	Used to deselect all the entries on a list, or all the ports on the device panel.
	Generally present on the configuration wizard; used to buffer but not apply the configuration of the current step and enter the next configuration step.
	Generally present on the configuration wizard; used to buffer but not apply the configuration of the current step and return to the previous configuration step.
	Generally present on the configuration wizard; used to apply the configurations of all configuration steps.
	Generally present on the "Operation" column on a list; used to enter the modification page of an item so that you can modify the configurations of the item.
	Generally present on the "Operation" column on a list; used to delete the item corresponding to this icon.
	Click the plus sign before a corresponding item. You can see the collapsed contents.

Page display

The web interface can display a long list by pages, as shown in [a](#). You can set the number of entries displayed per page, and use the **First**, **Prev**, **Next**, and **Last** links to view the contents on the first, previous, next, and last pages, or go to any page that you want to view.

a. Content display by pages

▶ Search Item: IP Address ▼ Keywords: Search

<input type="checkbox"/>	IP Address	MAC Address	VLAN ID	Port	Type	Operation
<input type="checkbox"/>	192.168.1.11	000d-88f7-f536	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.16	0019-2146-ca29	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.40	0000-000f-0008	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.41	0000-000f-0005	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.42	0000-000f-0011	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.43	000f-e23e-b583	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.45	000f-e23e-9ca5	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.46	000f-e240-a1a9	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.47	000f-e23e-fa3d	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.49	0000-000f-000b	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.55	000f-e2a3-76b3	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.56	000f-e26a-58ee	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.57	000f-e249-8048	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.58	000f-e258-b140	999	GigabitEthernet1/0/19	Dynamic	

14 records, 15 ▼ per page | page 1/1, record 1-14 | First Prev Next Last 1 GO

Search function

On some list pages, the web interface provides basic and advanced search functions. You can use the search function to display those entries matching certain search criteria.

- Basic search function—Select a search item from the drop-down list as shown in a, input the keyword, and click the **Query** button to display the entries that match the criteria.
- Advanced search function—Click ▶ before **Search Item**, as shown in a. You can select **Match case and whole word**, that is, the item to be searched must completely match the keyword, or you can select **Search in previous results**. If you do not select exact search, a fuzzy search is performed.

a. Advanced search

▼ Search Item: IP Address ▼ Keywords: Search

Match case and whole word















Search in previous results

Sorting function

On some list pages, the web interface provides the sorting function to display the entries in a certain order.

As shown in a, you can click the blue heading item of each column to sort the entries based on the heading item you selected. Then, the heading item is displayed with an arrow beside it. The upward arrow indicates the ascending order, and the downward arrow indicates the descending order.

a. Sort display (based on MAC address in the ascending order)

<input type="checkbox"/>	IP Address	MAC Address↑	VLAN ID	Port	Type	Operation
<input type="checkbox"/>	192.168.1.41	0000-000f-0005	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.40	0000-000f-0008	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.49	0000-000f-000b	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.42	0000-000f-0011	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.11	000d-88f7-f536	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.45	000f-e23e-9ca5	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.43	000f-e23e-b583	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.47	000f-e23e-fa3d	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.46	000f-e240-a1a9	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.57	000f-e249-8048	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.58	000f-e258-b140	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.56	000f-e26a-58ee	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.55	000f-e2a3-76b3	999	GigabitEthernet1/0/19	Dynamic	
<input type="checkbox"/>	192.168.1.16	0019-2146-ca29	999	GigabitEthernet1/0/19	Dynamic	

Configuration guidelines

- The web console supports Microsoft Internet Explorer 6.0 SP2 and higher.
- The web console does not support the **Back**, **Next**, **Refresh** buttons provided by the browser. Using these buttons may result in abnormal display of web pages.
- When the device is performing the spanning tree calculation, you cannot log in to or use the web interface.
- The Windows firewall limits the number of TCP connections, so when you use IE to log in to the web interface, sometimes you may be unable to open the web interface. To avoid this problem, turn off the Windows firewall before login.
- If the software version of the device changes, when you log in to the device through the web interface, delete the temporary Internet files of IE; otherwise, the web page content may not be displayed correctly.

Configuration at the CLI

NOTE:

- The HP V1910 Switch Series can be configured through the CLI, web interface, and SNMP/MIB, among which the web interface supports all V1910 Switch Series configurations. These configuration methods are suitable for different application scenarios. As a supplementary to the web interface, the CLI provides some configuration commands to facilitate your operation, which are described in this chapter. To perform other configurations not supported by the CLI, use the web interface.
 - You will enter user view directly after you log in to the device. Commands in the document are all performed in user view.
-

Getting started with the CLI

As a supplementary to the web interface, the CLI provides some configuration commands to facilitate your operation. For example, if you forget the IP address of VLAN-interface 1 and cannot log in to the device through the web interface, you can connect the console port of the device to a PC, and reconfigure the IP address of VLAN-interface 1 at the CLI.

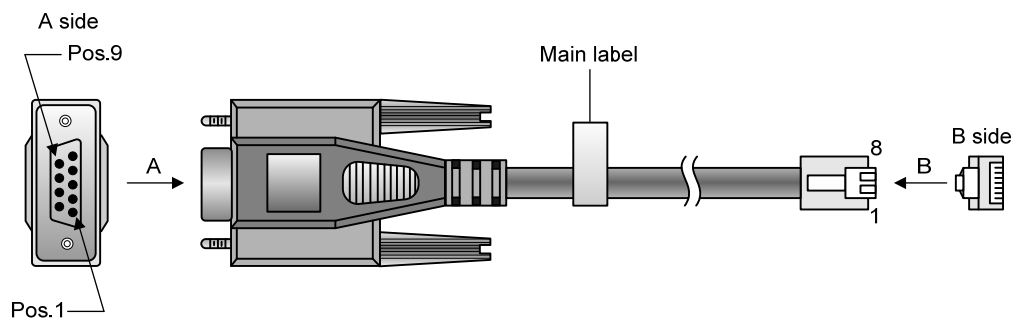
This section describes using the CLI to manage the device.

Setting up the configuration environment

To set up the configuration environment, connect a terminal (a PC in this example) to the console port on the switch with a console cable.

A console cable is an 8-core shielded cable, with a crimped RJ-45 connector at one end for connecting to the console port of the switch, and a DB-9 female connector at the other end for connecting to the serial port on the console terminal.

a. Console cable

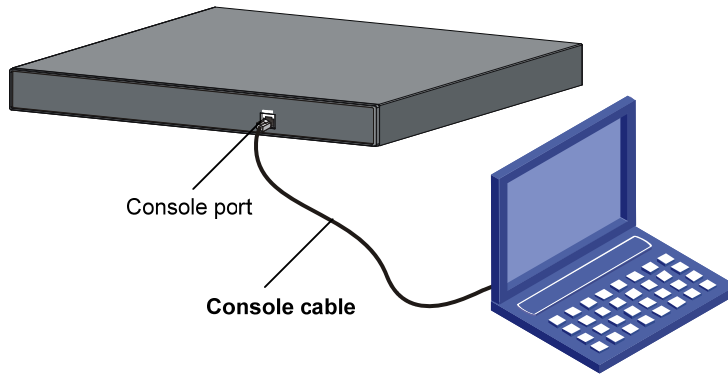


Use a console cable to connect a terminal device to the switch, as follows:

Table 3 Plug the DB-9 female connector to the serial port of the console terminal or PC.

Table 4 Connect the RJ-45 connector to the console port of the switch.

b. Network diagram for configuration environment setup



△ CAUTION:

Verify the mark on the console port to ensure that you are connecting to the correct port.

NOTE:

The serial port on a PC does not support hot swapping. When you connect a PC to a powered-on switch, connect the DB-9 connector of the console cable to the PC before connecting the RJ-45 connector to the switch.

- When you disconnect a PC from a powered-on switch, disconnect the DB-9 connector of the console cable from the PC after disconnecting the RJ-45 connector from the switch.
-

Setting terminal parameters

To configure and manage the switch, you must run a terminal emulator program on the console terminal, for example, a PC. This section uses Windows XP HyperTerminal as an example.

The following are the required terminal settings:

- Bits per second—38400
- Data bits—8
- Parity—None
- Stop bits—1
- Flow control—None
- Emulation—VT100

Follow these steps to set terminal parameters, for example, on a Windows XP HyperTerminal:

Table 5 Select **Start** → **All Programs** → **Accessories** → **Communications** → **HyperTerminal**, and in the **Connection Description** dialog box that appears, type the name of the new connection in the **Name** text box and click **OK**.

b. Connection description of the HyperTerminal

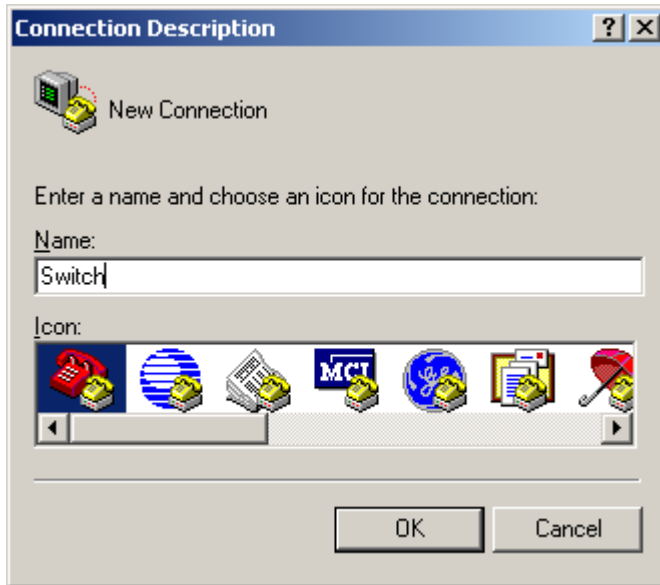


Table 6 Select the serial port to be used from the **Connect using** drop-down list, and click **OK**.

c. Set the serial port used by the HyperTerminal connection



Table 7 Set **Bits per second** to **38400**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, and click **OK**.

d. Set the serial port parameters

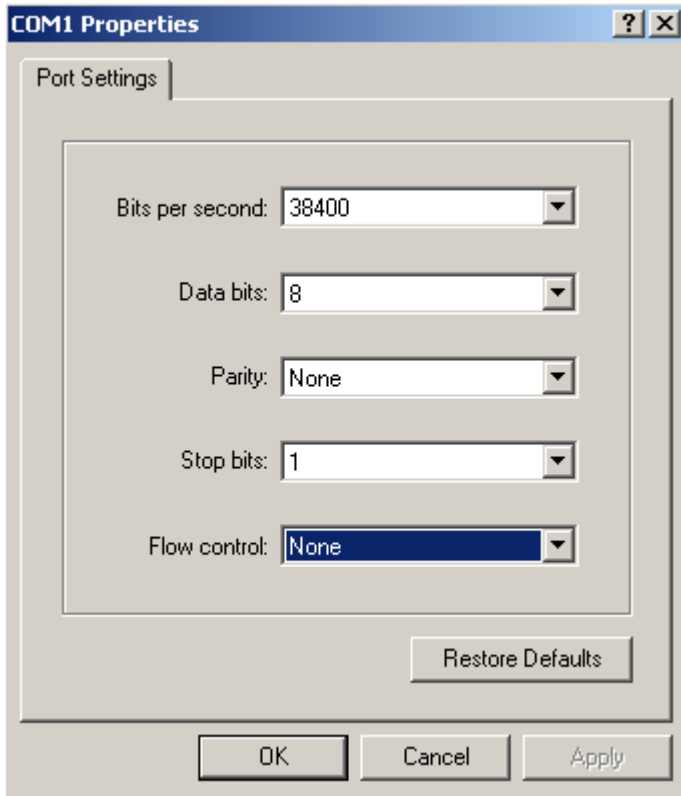


Table 8 Select **File** → **Properties** in the HyperTerminal window.

e. HyperTerminal window

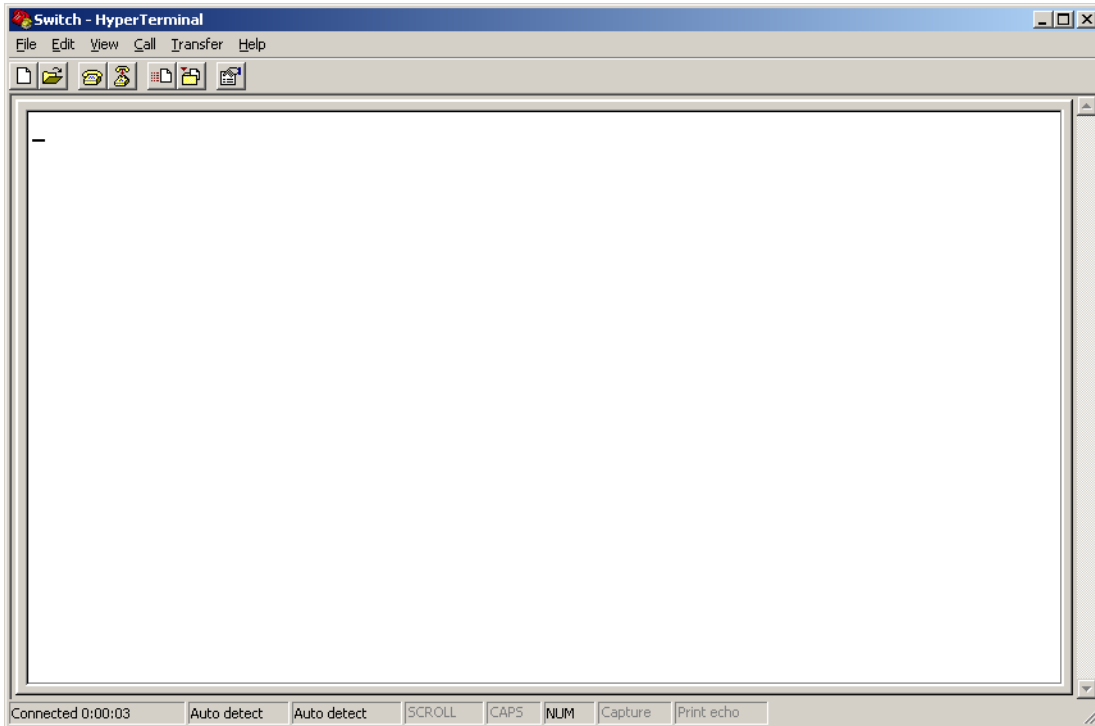
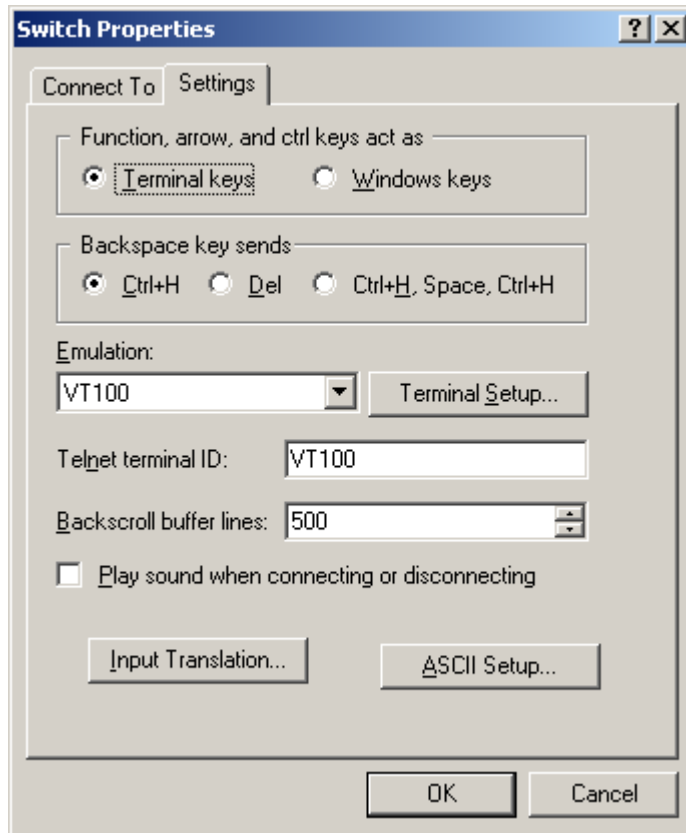


Table 9 Click the **Settings** tab, set the emulation to **VT100**, and click **OK** in the **Switch Properties** dialog box.

f. Set terminal emulation in Switch Properties dialog box



Logging in to the CLI

The login process requires a username and password. The default username for first time configuration is **admin**, no password is required. Usernames and passwords are case sensitive.

To log in to the CLI:

Table 10 Press **Enter**. The **Username** prompt displays:

```
Login authentication
```

```
Username:
```

Table 11 Enter your username at the **Username** prompt.

```
Username:admin
```

Table 12 Press **Enter**. The **Password** prompt display

```
Password:
```

The login information is verified, and displays the following CLI menu:

```
<HP V1910 Switch>
```

If the password is invalid, the following message appears and process restarts.

```
% Login failed!
```


CLI commands

This Command section contains the following commands:

To do...	Use the command...
Display a list of CLI commands on the device	?
Reboot the device and run the default configuration	initialize
Specify VLAN-interface 1 to obtain an IP address through DHCP or manual configuration	ipsetup { dhcp ip address <i>ip-address</i> { <i>mask</i> <i>mask-length</i> } [default-gateway <i>ip-address</i>] }
Modify the login password of a user	password
Download the Boot ROM image or system software image file from the TFTP server and specify as the startup configuration file	upgrade <i>server-address source-filename</i> { bootrom runtime }
Reboot the device and run the main configuration file	reboot
View the summary information of the device	summary
Ping a specified destination	ping <i>host</i>

initialize

Syntax

initialize

Parameters

None

Description

Use the **initialize** command to delete the current configuration file and reboot the device with the default configuration file.

Use the command with caution because it deletes the configuration file to be used at the next startup and restores the factory default settings.

Examples

```
# Delete the configuration file to be used at the next startup and reboot the device with the default configuration being used during reboot.
```

```
<Sysname> initialize
```

```
The startup configuration file will be deleted and the system will be rebooted.Continue?  
[Y/N]:y
```

```
Please wait...
```

ipsetup

Syntax

ipsetup { **dhcp** | **ip address** *ip-address* { *mask* | *mask-length* } [**default-gateway** *ip-address*] }

Parameters

dhcp: Specifies the interface to obtain an IP address through DHCP.

ip-address *ip-address*: Specifies an IP address for VLAN-interface 1 in dotted decimal notation.

mask: Subnet mask in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask, in the range of 0 to 32.

default-gateway *ip-address*: Specifies the IP address of the default gateway or the IP address of the outbound interface. With this argument and keyword combination configured, the command not only assigns an IP address to the interface, but also specifies a default route for the device.

Description

Use the **ipsetup dhcp** command to specify VLAN-interface 1 to obtain an IP address through DHCP.

Use the **ipsetup ip address** *ip-address* { *mask* | *mask-length* } command to assign an IP address to VLAN-interface 1.

By default, the device automatically obtains its IP address through DHCP; if fails, it uses the assigned default IP address. For more information, see [b](#).

If there is no VLAN-interface 1, either command creates VLAN-interface 1 first, and then specifies its IP address.

Examples

```
# Create VLAN-interface 1 and specify the interface to obtain an IP address through DHCP.
```

```
<Sysname> ipsetup dhcp
```

```
# Create VLAN-interface 1 and assign 192.168.1.2 to the interface, and specify 192.168.1.1 as the default gateway.
```

```
<Sysname> ipsetup ip-address 192.168.1.2 24 default-gateway 192.168.1.1
```

password

Syntax

```
password
```

Parameters

None

Description

Use the **password** command to modify the login password of a user.

Examples

```
# Modify the login password of user admin.
```

```
<Sysname> password
```

```
Change password for user: admin
```

```
Old password: ***
```

```
Enter new password: **
```

```
Retype password: **
```

```
The password has been successfully changed.
```

ping

Syntax

ping *host*

Parameters

host: Destination IP address (in dotted decimal notation), URL, or host name (a string of 1 to 20 characters).

Description

Use the **ping** command to ping a specified destination.

You can enter **Ctrl+C** to terminate a ping operation.

Examples

Ping IP address 1.1.2.2.

```
<Sysname> ping 1.1.2.2
  PING 1.1.2.2: 56 data bytes, press CTRL_C to break
    Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=205 ms
    Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 1.1.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/41/205 ms
```

The output shows that IP address 1.1.2.2 is reachable and the echo replies are all returned from the destination. The minimum, average, and maximum roundtrip intervals are 1 millisecond, 41 milliseconds, and 205 milliseconds respectively.

quit

Syntax

quit

Parameters

None

Description

Use the **quit** command to log out of the system.

Examples

Log out of the system.

```
<Sysname> quit
*****
* Copyright (c) 2004-2011 Hewlett-Packard Development Company, L.P.      *
* Without the owner's prior written consent,                             *
```

```
* no decompiling or reverse-engineering shall be allowed. *
*****
User interface aux0 is available.
```

Please press ENTER.

reboot

Syntax

reboot

Parameters

None

Description

Use the **reboot** command to reboot the device and run the main configuration file.

Use this command with caution because reboot results in service interruption.

If the main configuration file is corrupted or does not exist, the device cannot be rebooted with the **reboot** command. In this case, you can specify a new main configuration file to reboot the device, or you can power off the device, and then power it on, and the system will automatically use the backup configuration file at the next startup.

If you reboot the device when file operations are being performed, the system does not execute the command to ensure security.

Examples

If the configuration does not change, reboot the device.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.....DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

If the configuration changes, reboot the device.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.....DONE!
This command will reboot the device. Current configuration will be lost in next startup if
you continue. Continue? [Y/N]:y
Now rebooting, please wait...
```

summary

Syntax

summary

Parameters

None

Description

Use the **summary** command to view the summary information of the device, including the IP address of VLAN-interface 1, and software version information.

Examples

```
# Display summary information of the device.
```

```
<Sysname> summary
```

```
Select menu option:          Summary
IP Method:                   DHCP
IP address:                   10.153.96.86
Subnet mask:                  255.255.255.0
Default gateway:              0.0.0.0
```

```
Current boot app is: flash:/v1910-cmw520-a1108.bin
```

```
Next main boot app is: flash:/v1910-cmw520-a1108.bin
```

```
Next backup boot app is: NULL
```

```
HP Comware Platform Software
Comware Software, Version 5.20 Alpha 1108,
Copyright (c) 2004-2011 Hewlett-Packard Development Company, L.P.
HP V1910-24G-PoE (365W) Switch uptime is 0 week, 0 day, 6 hours, 28 minutes
```

```
HP V1910-24G-PoE (365W) Switch
128M   bytes DRAM
128M   bytes Nand Flash Memory
Config Register points to Nand Flash
```

```
Hardware Version is REV.B
CPLD Version is 002
Bootrom Version is 138
[SubSlot 0] 24GE+4SFP+POE Hardware Version is REV.B
```

upgrade

Syntax

```
upgrade server-address source-filename { bootrom | runtime }
```

Parameters

server-address: IP address or host name (a string of 1 to 20 characters) of a TFTP server.

source-filename: Software package name on the TFTP server.

bootrom: Specifies the Boot ROM image in the software package file as the startup configuration file.

runtime: Specifies the system software image file in the software package file as the startup configuration file.

Description

Use the **upgrade** *server-address source-filename bootrom* command to upgrade the Boot ROM image. If the Boot ROM image in the downloaded software package file is not applicable, the original Boot ROM image is still used as the startup configuration file.

Use the **upgrade** *server-address source-filename runtime* command to upgrade the system software image file. If the system software image file in the downloaded software package file is not applicable, the original system software image file is still used as the startup configuration file.

To make the downloaded software package file take effect, reboot the device.

NOTE:

The HP V1910 Switch Series does not provide an independent Boot ROM image; instead, it integrates the Boot ROM image with the system software image file together in a software package file with the extension name of **.bin**.

Examples

Download software package file **main.bin** from the TFTP server and use the Boot ROM image in the package as the startup configuration file.

```
<Sysname> upgrade 192.168.20.41 main.bin bootrom
```

Download software package file **main.bin** from the TFTP server and use the system software image file in the package as the startup configuration file.

```
<Sysname> upgrade 192.168.20.41 main.bin runtime
```

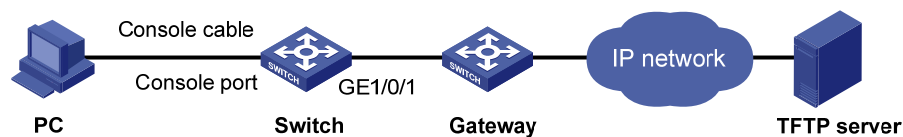
Configuration example for upgrading the system software image at the CLI

Network requirements

As shown in [a](#), a V1910 switch is connected to the PC through the console cable, and connected to the gateway through GigabitEthernet 1/0/1. The IP address of the gateway is 192.168.1.1/24, and the TFTP server where the system software image (**SwitchV1910.bin**) is located is 192.168.10.1/24. The gateway and the switch can reach each other.

The administrator upgrades the Boot ROM image and the system software image file of the V1910 switch through the PC and sets the IP address of the switch to 192.168.1.2/24.

a. Network diagram for upgrading the system software image of the V1910 switch at the CLI



Configuration procedure

Table 13 Run the TFTP server program on the TFTP server, and specify the path of the file to be loaded.
(Omitted)

Table 14 Perform the following configurations on the switch.

Configure the IP address of VLAN-interface 1 of the switch as 192.168.1.2/24, and specify the default gateway as 192.168.1.1.

```
<Switch> ipsetup ip-address 192.168.1.2 24 default-gateway 192.168.1.1
```

Download the software package file **SwitchV1910.bin** from the TFTP server to the switch, and upgrade the system software image in the package.

```
<Switch> upgrade 192.168.10.1 SwitchV1910.bin runtime
File will be transferred in binary mode
Downloading file from remote TFTP server, please wait.../
TFTP: 10262144 bytes received in 71 second(s)
File downloaded successfully.
```

Download the software package file **SwitchV1910.bin** from the TFTP server to the switch, and upgrade the Boot ROM image.

```
<Switch> upgrade 192.168.10.1 SwitchV1910.bin bootrom
The file flash:/SwitchV1910.bin exists. Overwrite it? [Y/N]:y
Verifying server file...
Deleting the old file, please wait...
File will be transferred in binary mode
Downloading file from remote TFTP server, please wait.../
TFTP: 10262144 bytes received in 61 second(s)
File downloaded successfully.
BootRom file updating finished!
```

Reboot the switch.

```
<Switch> reboot
```

After getting the new image file, reboot the switch to have the upgraded image take effect.

Configuration wizard

Overview

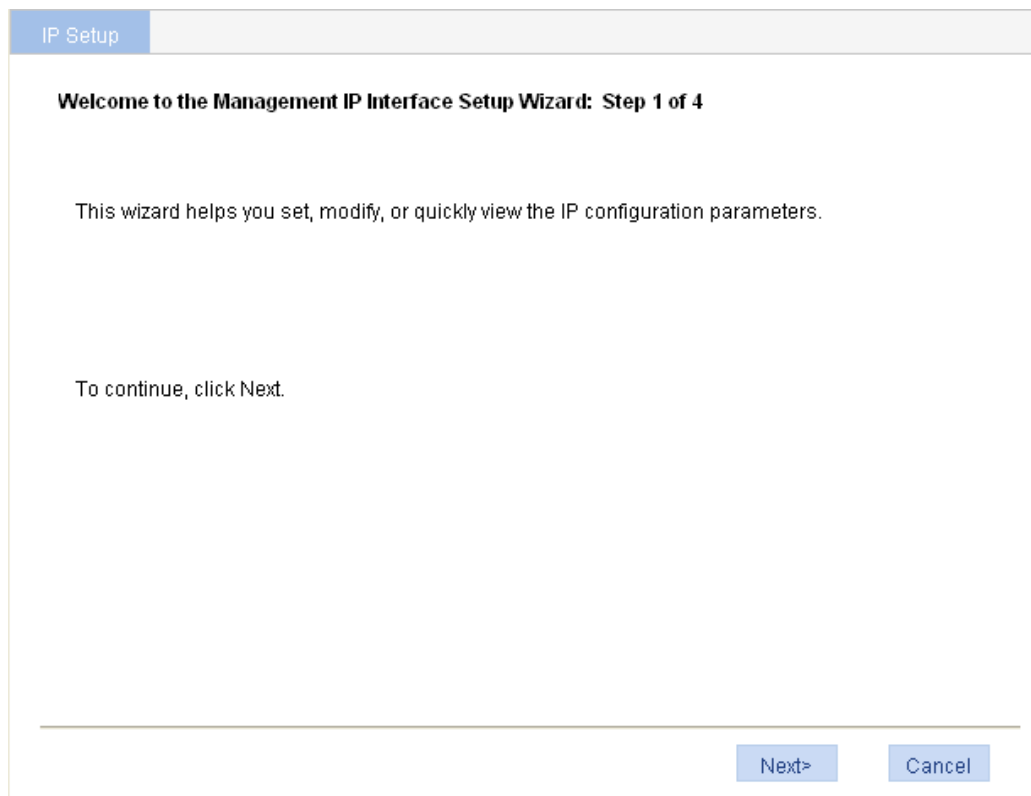
The configuration wizard guides you through the basic service setup, including the system name, system location, contact information, and management IP address (IP address of the VLAN interface).

Basic service setup

Entering the configuration wizard homepage

From the navigation tree, select **Wizard** to enter the configuration wizard homepage, as shown in a.

a. **Configuration wizard homepage**



Configuring system parameters

In the wizard homepage, click **Next** to enter the system parameter configuration page, as shown in a.

a. System parameter configuration page

IP Setup

System Parameters: Step 2 of 4

Sysname: (1- 30Char.)

Syslocation: (1- 200Char.)

Syscontact: (1- 200Char.)

<Back Next> Cancel

2. System parameter configuration items

Item	Description
Sysname	Specify the system name. The system name appears at the top of the navigation tree. You can also set the system name in the System Name page you enter by selecting Device → Basic . For more information, see the chapter "Device basic information configuration".
Syslocation	Specify the physical location of the system. You can also set the physical location in the setup page you enter by selecting Device → SNMP . For more information, see the chapter "SNMP configuration".
Syscontact	Set the contact information for users to get in touch with the device vendor for help. You can also set the contact information in the setup page you enter by selecting Device → SNMP . For more information, see the chapter "SNMP configuration".

Configuring management IP address

NOTE:

Modifying the management IP address used for the current login will tear down the connection to the device. Use the new management IP address to re-log in to the system.

A management IP address is the IP address of a VLAN interface, which can be used to access the device. You can also set configure a VLAN interface and its IP address in the page you enter by selecting **Network** → **VLAN Interface**. For more information, see the chapter “VLAN interface configuration”.

After finishing the configuration, click **Next** to enter the management IP address configuration page, as shown in a.

a. Management IP address configuration page

The screenshot shows a web-based configuration interface titled "IP Setup". The main heading is "Management IP Interface configuration: Step 3 of 4". Below this, a note states: "The IP address of a VLAN interface can be used as the management IP address to access the device." The configuration fields include:

- "Select VLAN Interface:" with a dropdown menu showing "1".
- "Admin status:" with a dropdown menu showing "Up".
- A section titled "Configure IPv4 address" which is checked. It contains three radio buttons: "DHCP", "BOOTP", and "Manual" (which is selected).
- "IPv4 address:" with a text input field containing "192.168.0.27".
- "MaskLen:" with a dropdown menu showing "24 (255.255.255.0)".

 At the bottom of the form are three buttons: "<Back", "Next>", and "Cancel".

2. Management IP address configuration items

Item	Description
Select VLAN Interface	Select a VLAN interface. Available VLAN interfaces are those configured in the page you enter by selecting Network → VLAN Interface and selecting the Create tab.
Admin Status	Enable or disable the VLAN interface. When errors occurred on the VLAN interface, disable the interface and then enable the port to bring the port to work properly. By default, the VLAN interface is in the down state if all Ethernet ports in the VLAN are down. The VLAN is in the up state if one or more ports in the VLAN are up. ! IMPORTANT: Disabling or enabling the VLAN interface does not affect the status of the Ethernet ports in the VLAN. That is, the port status does not change with the VLAN interface status.
Configure IPv4 address	DHCP Configure how the VLAN interface obtains an IPv4 address. <ul style="list-style-type: none"> DHCP: Specifies the VLAN interface to obtain an IPv4 address by

Item	Description
BOOTP	DHCP.
Manual	<ul style="list-style-type: none"> • BOOTP: Specifies the VLAN interface to obtain an IPv4 address through BOOTP. • Manual: Allows you to specify an IPv4 address and a mask length. <p>! IMPORTANT:</p> <p>Support for IPv4 obtaining methods depends on the device model.</p>
IPv4 address	Specify an IPv4 address and the mask length for the VLAN interface.
MaskLen	These two text boxes are configurable if Manual is selected.

Finishing configuration wizard

After finishing the management IP address configuration, click **Next**, as shown in [a](#).

a. Configuration finishes

IP Setup

Completing the Management IP Interface Setup Wizard: Step 4 of 4

You have successfully completed the Management IP Interface Setup wizard.

You have specified the following settings:

```

Sysname: HP V1910 Switch
Syslocation: HP
Syscontact: http://www.hp.com

VLAN Interface: 1      Admin Status: UP

Config IPv4 address:
Method: Manual
IPv4 address: 192.168.0.27
Subnet mask: 255.255.255.0

```

<Back
Finish
Cancel

The page displays your configurations. Review the configurations and if you want to modify the settings click **Back** to go back to the page. Click **Finish** to confirm your settings and the system then performs the configurations.

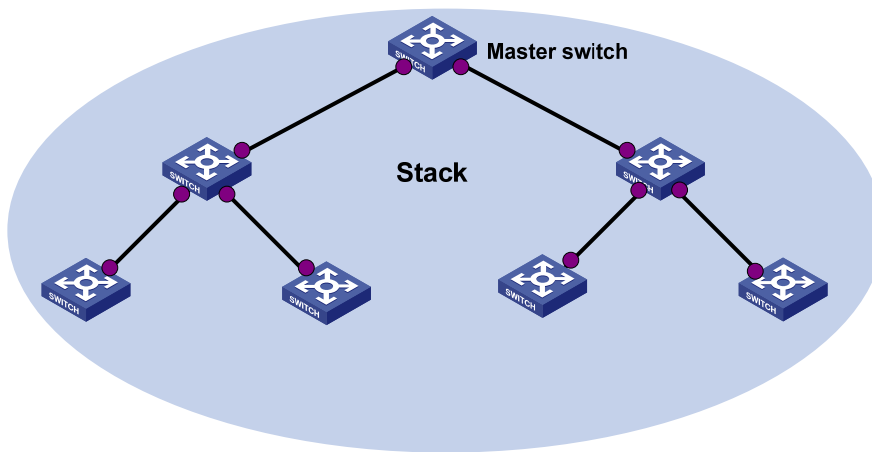
IRF stack management

The HP V1910 IRF stack management feature enables you to configure and monitor a stack of connected HP V1910 switches by logging in to one switch in the stack, as shown in a.

! **IMPORTANT:**

The HP V1910 IRF stack management feature does not provide the functions of HP Intelligent Resilient Framework (IRF) technology. To avoid confusion, IRF stack management is simply called stack management in this document.

a. Network diagram for stack management



To set up a stack, you must log in to one switch to create the stack, and this switch becomes the master for the stack. You then configure and monitor all other member switches on the master switch. The ports that connect the stack member switches are called stack ports.

Configuring stack management

Stack management configuration task list

Perform the tasks in 1 to configure stack management.

1. Stack management configuration task list

Task	Remarks
Configuring the master switch of a stack	Configuring global parameters of a stack
	Required
	Configure a private IP address pool for a stack and establish the stack, with the switch becoming the master switch of the stack.
	By default, no IP address pool is configured for a stack and no stack is established.

Task	Remarks
Configuring stack ports	Required Configure the ports of the master switch that connect to member switches as stack ports. By default, a port is not a stack port.
Configuring member switches of a stack Configuring stack ports	Required Configure a port of a member switch that connects to the master switch or another member switch as a stack port. By default, a port is not a stack port.
Displaying topology summary of a stack	Optional Display the information of stack members.
Displaying device summary of a stack	Optional Display the control panels of stack members. ! IMPORTANT: Before viewing the control panel of a member switch, you must ensure that the username, password, and access right you used to log on to the master switch are the same with those configured on the member switch; otherwise, the control panel of the member switch cannot be displayed.
Logging into a member switch from the master switch	Optional Log in to the web interface of a member switch from the master switch. ! IMPORTANT: Before logging into a member switch, you must ensure that the username, password, and access right you used to log on to the master switch are the same with those configured on the member switch; otherwise, you cannot log into the member switch. You can configure them by selecting Device and then clicking Users from the navigation tree.

Configuring global parameters of a stack

Select **IRF** from the navigation tree to enter the page shown in [a](#). You can configure global parameters of a stack in the **Global Settings** area.

a. Setup

Setup	Topology Summary	Device Summary
-------	------------------	----------------

Global Settings

Private Net IP Mask

Build Stack

Port Settings

▶ Search Item: Keywords:

<input type="checkbox"/>	Port Name	Port Status
<input type="checkbox"/>	GigabitEthernet1/0/1	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/2	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/3	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/4	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/5	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/6	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/7	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/8	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/9	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/10	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/11	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/12	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/13	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/14	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/15	not stack port

20 records, per page | page 1/2, record 1-15 |

2. Configuration items of global parameters

Item	Description
Private Net IP	<p>Configure a private IP address pool for the stack.</p> <p>The master switch of a stack must be configured with a private IP address pool to ensure that it can automatically allocate an available IP address to a member switch when the device joins the stack.</p>
Mask	<p>! IMPORTANT:</p> <p>When you configure a private IP address pool for a stack, the number of IP addresses in the address pool needs to be equal to or greater than the number of switches to be added to the stack. Otherwise, some switches may not be able to join the stack automatically for lack of private IP addresses.</p>

Item	Description
Build Stack	<p>Enable the switch to establish a stack.</p> <p>After you enable the switch to establish a stack, the switch becomes the master switch of the stack and automatically adds the switches connected to its stack ports to the stack.</p> <p>! IMPORTANT:</p> <p>You can delete a stack only on the master switch of the stack. The Global Settings area on a member switch is grayed out.</p>

Return to [Stack management configuration task list](#).

Configuring stack ports

Select **IRF** from the navigation tree to enter the page shown in [a](#). You can configure stack ports in the **Port Settings** area.

- Select the check box before a port name, and click **Enable** to configure the port as a stack port.
- Select the check box before a port name, and click **Disable** to configure the port as a non-stack port.

Return to [Stack management configuration task list](#).

Displaying topology summary of a stack

Select **IRF** from the navigation tree and click the **Topology Summary** tab to enter the page shown in [a](#).

a. Topology summary

Setup	Topology Summary	Device Summary							
	<table border="1"> <thead> <tr> <th>Member ID</th> <th>Role</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Slave</td> </tr> <tr> <td>0</td> <td>Master</td> </tr> </tbody> </table>	Member ID	Role	1	Slave	0	Master		
Member ID	Role								
1	Slave								
0	Master								

2. Fields of topology summary

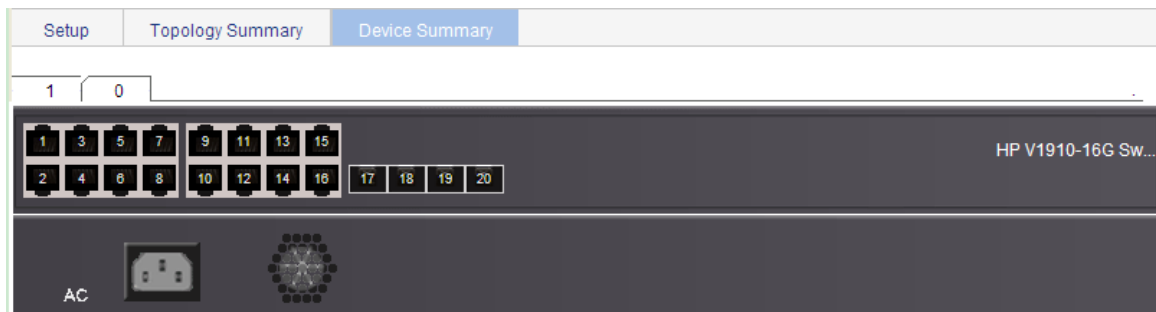
Fields	Description
Member ID	<p>Member ID of the device in the stack:</p> <ul style="list-style-type: none"> • Value 0 indicates that the switch is the master switch of the stack. • A value other than 0 indicates that the switch is a member switch and the value is the member ID of the switch in the stack.
Role	Role of the switch in the stack: master or member.

Return to [Stack management configuration task list](#).

Displaying device summary of a stack

Select **IRF** from the navigation tree and click the **Device Summary** tab to enter the page shown in [a](#). On this page, you can view interfaces and power socket layout on the panel of each stack member by clicking the tab of the corresponding member switch.

a. Device summary (the master switch)



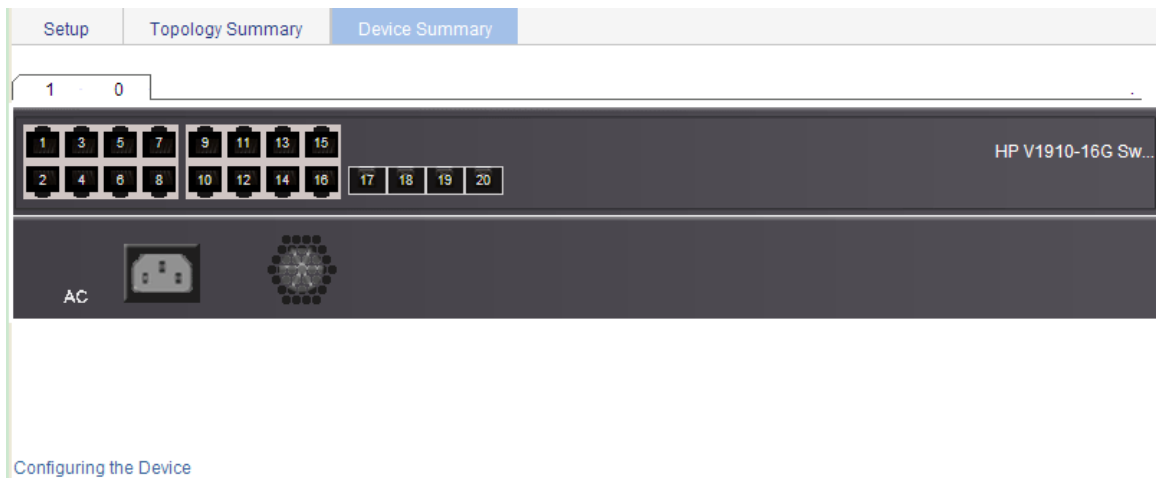
Return to [Stack management configuration task list](#).

Logging into a member switch from the master switch

Select **IRF** from the navigation tree, click the **Device Summary** tab, and click the tab of a member switch to enter the page shown in [a](#).

Click the **Configuring the Device** hyperlink, you can log on to the web interface of the member switch to manage and maintain the member switch directly.

a. Device summary (a member switch)



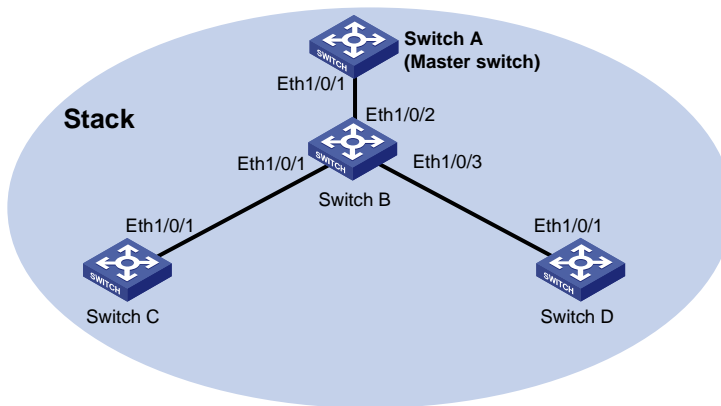
Return to [Stack management configuration task list](#).

Stack configuration example

Network requirements

- As shown in [a](#), Switch A, Switch B, Switch C, and Switch D are connected with one another.

- Create a stack, where Switch A is the master switch, Switch B, Switch C, and Switch D are stack members. An administrator can log in to Switch B, Switch C and Switch D through Switch A to perform remote configurations.
- a. **Network diagram for stack management**



Configuration procedure

Table 15 Configure the master switch

Configure global parameters for the stack on Switch A.

- Select **IRF** from the navigation tree of Switch A to enter the page of the **Setup** tab.

b. Configure global parameters for the stack on Switch A

Setup | Topology Summary | Device Summary

Global Settings

Private Net IP: 192.168.1.1 Mask: 255.255.255.0
Build Stack: Enable
Apply

Port Settings

Search Item: Port Name Keywords: Search

<input type="checkbox"/>	Port Name	Port Status
<input type="checkbox"/>	GigabitEthernet1/0/1	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/2	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/3	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/4	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/5	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/6	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/7	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/8	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/9	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/10	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/11	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/12	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/13	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/14	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/15	not stack port

20 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Enable Disable

- Type **192.168.1.1** in the text box of **Private Net IP**.
- Type **255.255.255.0** in the text box of **Mask**.
- Select **Enable** from the **Build Stack** drop-down list.
- Click **Apply**.

Now, switch A becomes the master switch.

Configure a stack port on Switch A.

- On the page of the **Setup** tab, perform the following configurations, as shown in c.

c. **Configure a stack port on Switch A**

Setup | Topology Summary | Device Summary

Global Settings

Private Net IP: Mask:

Build Stack:

Port Settings

Search Item: Keywords:

<input type="checkbox"/>	Port Name	Port Status
<input checked="" type="checkbox"/>	GigabitEthernet1/0/1	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/2	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/3	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/4	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/5	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/6	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/7	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/8	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/9	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/10	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/11	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/12	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/13	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/14	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/15	not stack port

20 records, per page | page 1/2, record 1-15 |

- In the **Port Settings** area, select the check box before **GigabitEthernet1/0/1**.
- Click **Enable**.

Table 16 Configure the member switches

On Switch B, configure local ports GigabitEthernet 1/0/2 connecting with switch A, GigabitEthernet 1/0/1 connecting with Switch C, and GigabitEthernet 1/0/3 connecting with Switch D as stack ports.

- Select **IRF** from the navigation tree of Switch B to enter the page of the **Setup** tab.

d. Configure stack ports on Switch B

Setup Topology Summary Device Summary

Global Settings

Private Net IP Mask

Build Stack

Apply

Port Settings

Search Item: Keywords: Search

<input type="checkbox"/>	Port Name	Port Status
<input checked="" type="checkbox"/>	GigabitEthernet1/0/1	not stack port
<input checked="" type="checkbox"/>	GigabitEthernet1/0/2	not stack port
<input checked="" type="checkbox"/>	GigabitEthernet1/0/3	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/4	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/5	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/6	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/7	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/8	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/9	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/10	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/11	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/12	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/13	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/14	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/15	not stack port

20 records, per page | page 1/2, record 1-15 | First Prev Next Last GO

Enable Disable

- In the **Port Settings** area, select the check boxes before **GigabitEthernet1/0/1**, **GigabitEthernet1/0/2**, and **GigabitEthernet1/0/3**.
- Click **Enable**.

Now, switch B becomes a member switch.

On Switch C, configure local port GigabitEthernet 1/0/1 connecting with Switch B as a stack port.

- Select **IRF** from the navigation tree of Switch C to enter the page of the **Setup** tab.

e. **Configure a stack port on Switch C**

Setup | Topology Summary | Device Summary

Global Settings

Private Net IP Mask

Build Stack

Apply

Port Settings

Search Item: Keywords: Search

<input type="checkbox"/>	Port Name	Port Status
<input checked="" type="checkbox"/>	GigabitEthernet1/0/1	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/2	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/3	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/4	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/5	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/6	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/7	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/8	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/9	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/10	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/11	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/12	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/13	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/14	not stack port
<input type="checkbox"/>	GigabitEthernet1/0/15	not stack port

20 records, per page | page 1/2, record 1-15 | First Prev Next Last GO

Enable Disable

- In the **Port Settings** area, select the check box before **GigabitEthernet1/0/1**.
- Click **Enable**.

Now, Switch C becomes a member switch.

On Switch D, configure local port GigabitEthernet 1/0/1 connecting with Switch B as a stack port.

- Select **IRF** from the navigation tree of Switch D to enter the page of the **Setup** tab.
- In the **Port Settings** area, select the check box before **GigabitEthernet1/0/1**.
- Click **Enable**.

Now, Switch D becomes a member switch.

Table 17 Verify the configuration

Display the stack topology on Switch A.

- Select **IRF** from the navigation tree of Switch A and click the **Topology Summary** tab.
- You can view the information as shown in **f**.

f. Verify the configuration

Setup	Topology Summary	Device Summary	
Member ID	Role		
0	Master		
1	Slave		
2	Slave		
3	Slave		

Configuration guidelines

When configuring a stack, note the following issues:

Table 18 If a switch is already configured as the stack master, you are not allowed to modify the private IP address pool on the switch.

Table 19 If a switch is already configured as a stack member, the **Global Settings** area on the member switch is grayed out.

Summary

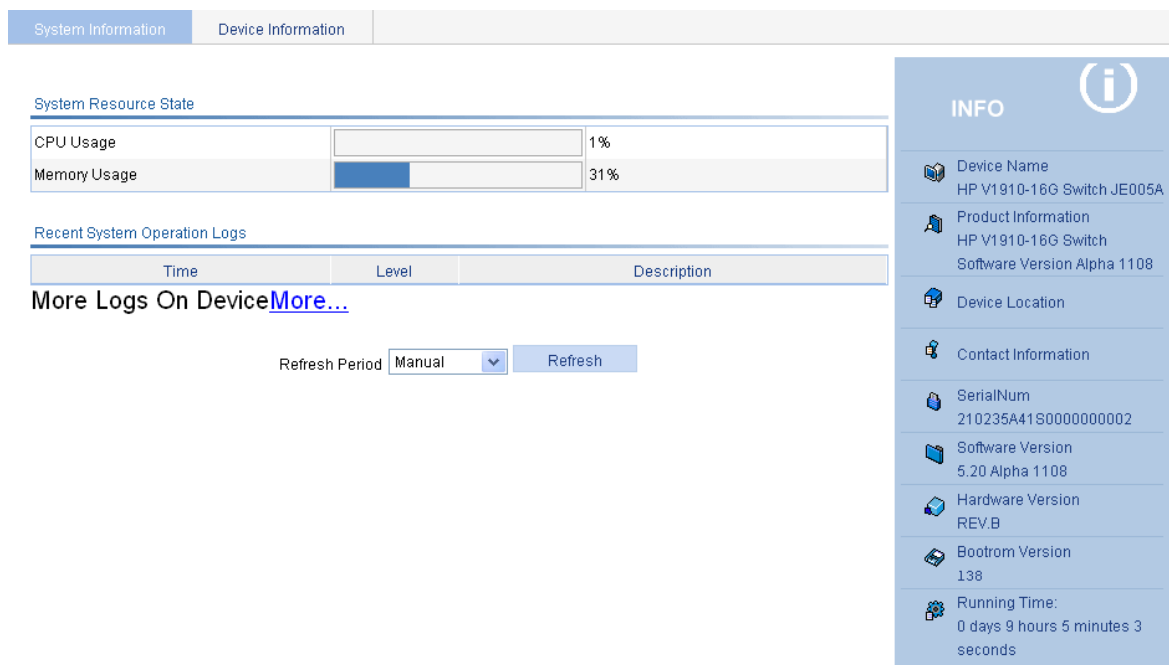
The device summary module helps you understand the system information, port information, power information, and fan information on the device. The system information includes the basic system information, system resources state, and recent system operation logs.

Displaying device summary

Displaying system information

After you log in to the web interface, the **System Information** tab appears by default, as shown in [a](#).

a. System information



Time	Level	Description
------	-------	-------------

Refresh Period:

INFO	
Device Name	HP V1910-16G Switch JE005A
Product Information	HP V1910-16G Switch Software Version Alpha 1108
Device Location	
Contact Information	
SerialNum	210235A41S0000000002
Software Version	5.20 Alpha 1108
Hardware Version	REV.B
Bootrom Version	138
Running Time:	0 days 9 hours 5 minutes 3 seconds

- If you select a certain time period, the system refreshes the system information at the specified interval.
- If you select **Manual** from the **Refresh Period** drop-down list, the system refreshes the information only when you click the **Refresh** button.

The system information tab is divided into three sections, which display the following information:

- [Basic system information](#)
- [System resource state](#)
- [Recent system operation logs](#)

Basic system information

The **INFO** area on the right of the page displays the basic system information such as device name, product information, device location, contact information, serial number, software version, hardware version, Boot ROM version, and running time. The running time displays how long the device is up since the last boot.

You can configure the device location and contact information on the **Setup** page you enter by selecting **Device** → **SNMP**.

System resource state

The System Resource State displays the latest CPU usage and memory usage.

Recent system operation logs

1. Description about the recent system operation logs

Field	Description
Time	Displays the time when the system operation logs are generated.
Level	Displays the severity of the system operation logs.
Description	Displays the description of the system operation logs.

NOTE:

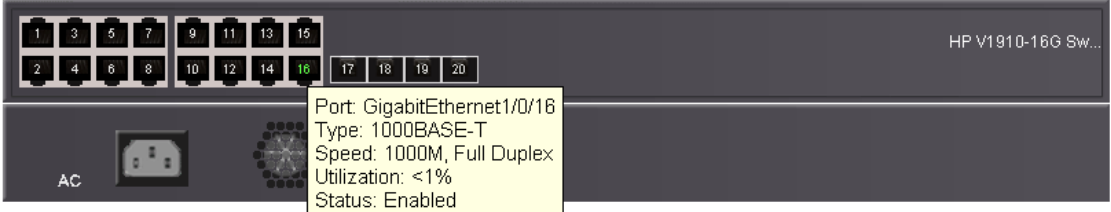
- The **Summary** page displays up to five latest system operation logs about the login and logout events.
- For more system operation logs, click **More** to enter the **Log List** page. You can also enter this page by selecting **Device** → **Syslog**. For more information, see the chapter “Log management configuration”.

Displaying device information

After logging in to the web interface, you can click the **Device Information** tab to enter the page displaying the device ports. Hover the cursor over a port and the port details appears, including the port name, type, speed, utilization, and status, as shown in [a](#). For the description about the port number and its color, see [a](#). Similarly, you can view the power type and working status and the fan working status.

a. Device information

System Information Device Information







HP V1910-16G Sw...

Port: GigabitEthernet1/0/16
Type: 1000BASE-T
Speed: 1000M, Full Duplex
Utilization: <1%
Status: Enabled

Refresh Period 30 seconds Refresh

Description of port number color:

-  Unconnected Port.
-  Connected port.
-  Port that has been set to inactive by user or protocol.
-  Port that has been selected by user.

Description on port numbers:

- Common number: Number of the port
 - Underlined number: Number of the aggregation group of the port
- If you select a certain time period from the **Refresh Period** drop-down list, the system refreshes the information at the specified interval.
 - If you select **Manual** from the **Refresh Period** drop-down list, the system refreshes the information only when you click the **Refresh** button.

Device basic information configuration

The device basic information feature provides the following functions:

- Set the system name of the device. The configured system name is displayed on the top of the navigation bar.
- Set the idle timeout period for logged-in users. The system logs an idle user off the web for security purpose after the configured period.

Configuring device basic information

Configuring system name

Select **Device** → **Basic** from the navigation tree to enter the system name configuration page, as shown in [a](#).

a. Configure system name

System Name Web Idle Timeout

Set sysname

Sysname * Chars.(1-30)

Items marked with an asterisk(*) are required

Apply

2. System name configuration item

Item	Description
Sysname	Set the system name.

Configuring idle timeout period

Select **Device** → **Basic** from the navigation tree, and then click the **Web Idle Timeout** tab to enter the page for configuring idle timeout period, as shown in [a](#).

a. Configure idle timeout period

System Name	Web Idle Timeout
-------------	------------------

Set idle timeout

Idle timeout *Minutes(1-999, Default = 10)

Items marked with an asterisk(*) are required

2. Idle timeout period configuration item

Item	Description
Idle timeout	Set the idle timeout period for logged-in users.

System time configuration

The system time module allows you to display and set the device system time on the web interface. The device supports setting system time through manual configuration and automatic synchronization of NTP server time.

An administrator can keep time synchronized among all the devices within a network by changing the system clock on each device, however, this is a huge amount of workload and cannot guarantee the clock precision.

Defined in RFC 1305, the Network Time Protocol (NTP) synchronizes timekeeping among distributed time servers and clients. NTP allows quick clock synchronization within the entire network and ensures a high clock precision so that the devices can provide diverse applications based on the consistent time.

Configuring system time

Select **Device** → **System Time** from the navigation tree. The system time configuration page appears by default, as shown in a. The current system time and clock status are displayed.

a. System time configuration page

The screenshot shows the 'System Time Configuration' page. At the top, there is a 'System Time' tab. Below it, the current system time is displayed as '2000-04-26 13:19:29' with a 'Refresh' button. The clock status is 'unsynchronized'. The main configuration area is titled 'Configure the system time' and has two radio buttons: 'Manual' (unselected) and 'NTP' (selected). Under 'Manual', there are dropdown menus for Hour (13), Minute (19), Second (29), Month (4), Date (26), and Year (2000). Under 'NTP', there is a 'Source Interface' dropdown set to 'Vlan-interface1'. Below that are two rows for 'Key 1' and 'Key 2', each with an 'ID' field (placeholder '(1-4294967295)') and a 'Key String' field (placeholder '(1-32 Chars)'). An 'External Reference Source' section contains two rows for 'NTP Server 1' and 'NTP Server 2', each with an ID field and a 'Reference Key' field. At the bottom, there is a 'Set System TimeZone' section with a 'TimeZone' dropdown set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. An 'Apply' button is located at the bottom center.

2. System time configuration items

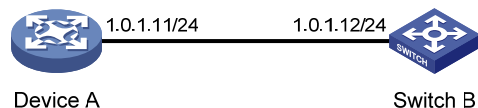
Item	Description				
Manual	Select to manually configure the system time, including the setting of Year, Month, Day, Hour, Minute, and Second .				
Source Interface	Set the source interface for an NTP message. If you do not want the IP address of a certain interface on the local device to become the destination address of response messages, you can specify the source interface for NTP messages, so that the source IP address in the NTP messages is the primary IP address of this interface.				
Key 1	Set an NTP authentication key. The NTP authentication feature should be enabled for a system running NTP in a network where there is a high security demand. This feature enhances the network security by means of client-server key authentication, which prohibits a client from synchronizing with a device that has failed authentication.				
Key 2	You can set two authentication keys, each of which is composed of a key ID and key string. <ul style="list-style-type: none"> • ID is the ID of a key. • Key string is a character string for MD5 authentication key. 				
NTP					
External Reference Source	<table border="1"> <tr> <td>NTP Server 1/Reference Key ID</td> <td>Specify the IP address of an NTP server, and configure the authentication key ID used for the association with the NTP server. Only if the key provided by the server is the same with the specified key will the device synchronize its time to the NTP server.</td> </tr> <tr> <td>NTP Server 2/Reference Key ID</td> <td>You can configure two NTP servers. The clients will choose the optimal reference source.</td> </tr> </table> <p>! IMPORTANT: The IP address of an NTP server is a unicast address, and cannot be a broadcast or a multicast address, or the IP address of the local clock source.</p>	NTP Server 1/Reference Key ID	Specify the IP address of an NTP server, and configure the authentication key ID used for the association with the NTP server. Only if the key provided by the server is the same with the specified key will the device synchronize its time to the NTP server.	NTP Server 2/Reference Key ID	You can configure two NTP servers. The clients will choose the optimal reference source.
NTP Server 1/Reference Key ID	Specify the IP address of an NTP server, and configure the authentication key ID used for the association with the NTP server. Only if the key provided by the server is the same with the specified key will the device synchronize its time to the NTP server.				
NTP Server 2/Reference Key ID	You can configure two NTP servers. The clients will choose the optimal reference source.				
TimeZone	Set the time zone for the system.				

System time configuration example

Network requirements

- As shown in a, the local clock of Device A is set as the reference clock.
- Switch B works in the client mode, and uses Device A as the NTP server.
- Configure NTP authentication on Device A and Switch B.

a. Network diagram for configuring system time



Configuration procedure

Table 20 Configure Device A

Configure the local clock as the reference clock, with the stratum of 2. Enable NTP authentication, set the key ID to **24**, and specify the created authentication key **aNiceKey** as a trusted key. (Configuration omitted.)

Table 21 Configure Switch B

Configure Device A as the NTP server of Switch B.

- Select **Device** → **System Time** from the navigation tree, and then select the **Net Time** tab to perform the configurations as shown in **b**.

b. Configure Device A as the NTP server of Switch B

System Time

System Time Configuration

System Time: 2000-04-26 13:46:11 Refresh

Clock status: unsynchronized

Configure the system time

Manual

Hour Minute Second

Month Date Year

NTP

Source Interface

Key 1	ID <input type="text" value="24"/>	(1-4294967295)	Key String <input type="text" value="aNiceKey"/>	(1-32 Chars.)
Key 2	ID <input type="text"/>	(1-4294967295)	Key String <input type="text"/>	(1-32 Chars.)

External Reference Source

NTP Server 1	<input type="text" value="1.0.1.11"/>	Reference Key ID <input type="text" value="24"/>
NTP Server 2	<input type="text"/>	Reference Key ID <input type="text"/>

Set System TimeZone

TimeZone:

Apply

- Select **NTP**.
- Type **24** in the **ID** box, and type **aNiceKey** in the **Key String** text box for key 1.
- Type **1.0.1.11** in the **NTP Server 1** text box and type **24** in the **Reference Key ID** text box.
- Click **Apply**.

Table 22 Verify the configuration

After the above configuration, you can see that the current system time on Device A is the same as Switch B.

Configuration guidelines

When configuring system time, note the following guidelines:

- A device can act as a server to synchronize the clock of other devices only after its clock has been synchronized. If the clock of a server has a stratum level higher than or equal to that of a client's clock, the client does not synchronize its clock to the server's.
- The synchronization process takes a period of time. Therefore, the clock status may be **unsynchronized** after your configuration. In this case, you can refresh the page to view the clock status and system time later on.

Log management configuration

System logs contain a large amount of network and device information, including running status and configuration changes. System logs are an important way for administrators to know network and device status. With system log information, administrators can take corresponding actions against network problems and security problems.

System logs can be stored in the log buffer, or sent to the loghost.

Configuring log management

Configuration task list

Perform the tasks in 1 to configure log management.

1. Log management configuration task list

Task	Description
Setting syslog related parameters	Optional <ul style="list-style-type: none">Set the number of logs that can be stored in the log buffer.Set the refresh period of the log information displayed on the web interface.
Displaying syslog	Display detailed information of system logs.
Setting loghost	Optional Set the loghost that can receive system logs.

Setting syslog related parameters

Select **Device** → **Syslog** from the navigation tree, and click the **Log Setup** tab to enter the syslog configuration page, as shown in [a](#).

a. Set system logs related parameters

Loglist	Loghost	Log Setup
<p>Buffer Set</p> <p>Buffer Capacity <input type="text" value="512"/> Item(s) (1 - 1024, default=512)</p>		
<p>Refresh Set</p> <p>Refresh Interval <input type="text" value="Manual"/></p>		
<p>Apply</p>		

2. Syslog configuration items

Item	Description
Buffer Capacity	Set the number of logs that can be stored in the log buffer.
Refresh Interval	<p>Set the refresh period on the log information displayed on the web interface.</p> <p>You can select manual refresh or automatic refresh:</p> <ul style="list-style-type: none">• Manual—Click Refresh to refresh the Web interface when displaying log information.• Automatic—Select a time period to refresh the Web interface every 1 minute, 5 minutes, or 10 minutes.

Return to [Log management configuration task list](#).

Displaying syslog

Select **Device** → **Syslog** from the navigation tree to enter the syslog display page, as shown in [a](#).

a. Display syslog

Loglist | Loghost | Log Setup

Search Item: Keywords:

Time/Date	Source	Level	Digest	Description
Apr 26 12:00:15:768 2000	MSTP	Critical	STPSTART	STP is now enabled on the device.
Apr 26 12:00:14:612 2000	HTTPD	Warning	Log	Start HTTP server.

Total: 2 Item(s)

2. Syslog display items

Item	Description
Time/Date	Displays the time/date when system logs are generated.
Source	Displays the module that generates system logs.
Level	Displays the severity level of system logs. For more information about severity levels, see 3.
Digest	Displays the brief description of system logs.
Description	Displays the contents of system logs.

3. System logs severity level

Severity level	Description	Value
Emergency	The system is unavailable.	0
Alert	Information that demands prompt reaction	1
Critical	Critical information	2
Error	Error information	3
Warning	Warnings	4
Notification	Normal information that needs to be noticed	5
Informational	Informational information to be recorded	6
Debugging	Information generated during debugging	7

Note: A smaller value represents a higher severity level.

Return to [Log management configuration task list](#).

Setting loghost

Select **Device** → **Syslog** from the navigation tree, and click the **Loghost** tab to enter the loghost configuration page, as shown in [a](#).

a. Set loghost

Loglist **Loghost** Log Setup

Loghost IP

Apply

Please select the loghost IP

Loghost	IP
---------	----

Select All Select None Remove

Note: The maximum number of loghosts that can be configured is 4.

2. Loghost configuration item

Item	Description
Loghost IP	IP address of the loghost. <ul style="list-style-type: none">You can specify up to four loghosts.You must input a valid IP address.

Return to [Log management configuration task list](#).

Configuration management

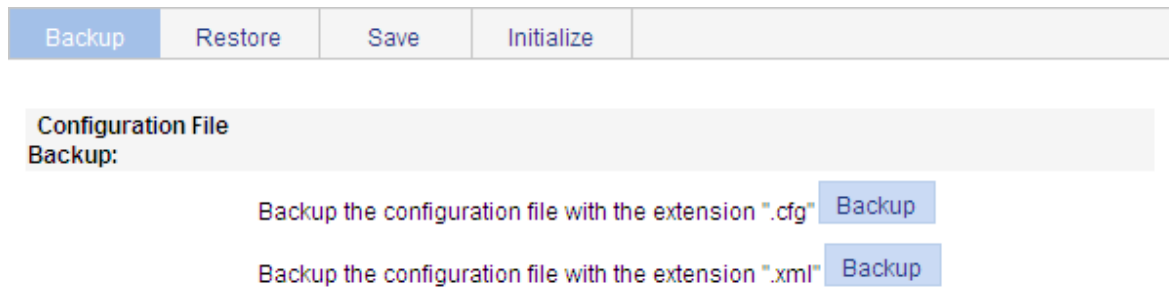
Back up configuration

Configuration backup provides the following functions:

- Open and view the configuration file (.cfg file or .xml file) for the next startup
- Back up the configuration file (.cfg file or .xml file) for the next startup to the host of the current user

Select **Device** → **Configuration** from the navigation tree to enter the backup configuration page, as shown in a.

a. Backup configuration page



- When you click the upper **Backup** button in this figure, a file download dialog box appears. You can select to view the .cfg file or to save the file locally.
- When you click the lower **Backup** button in this figure, a file download dialog box appears. You can select to view the .xml file or to save the file locally.

Restore configuration

Configuration restore provides the following functions:

- Upload the .cfg file on the host of the current user to the device for the next startup
- Upload the .xml file on the host of the current user to the device for the next startup, and delete the previous .xml configuration file that was used for the next startup

Select **Device** → **Configuration** from the navigation tree, and then click the **Restore** tab to enter the configuration restore page, as shown in a.

a. Configuration restore page

Backup	Restore	Save	Initialize	
--------	---------	------	------------	--

Restore the Configuration File:

(the file with the extension ".cfg")

(the file with the extension ".xml")

Note: The restored configuration will take effect after reboot.

Items marked with an asterisk(*) are required

- When you click the upper **Browse** button in this figure, the file upload dialog box appears. Select the **.cfg** file to be uploaded, and then click **OK**.
- When you click the lower **Browse** button in this figure, the file upload dialog box appears. Select the **.xml** file to be uploaded, and then click **OK**.

Save configuration

The save configuration module provides the function to save the current configuration to the configuration file (**.cfg** file or **.xml** file) for the next startup.

△ CAUTION:

- Saving the configuration takes some time.
- The system does not support the operation of saving configuration of two or more consecutive users. If such a case occurs, the system prompts the latter users to try later.

You can save the configuration in one of the following ways:

- Fast—Click the **Save** button at the upper right of the auxiliary area.
- Common—Select **Device** or **Configuration** from the navigation tree, and then click the **Save** tab to enter the save configuration confirmation page, as shown in a. Click **Save Current Settings**.

a. Save configuration confirmation

				Save Help Logout
Backup	Restore	Save	Initialize	

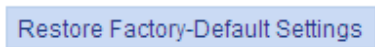
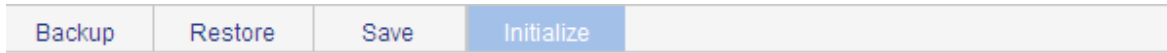
Note: Click **Save Current Settings** to save the current configuration.

Initialize

This operation restores the system to factory defaults, deletes the current configuration file, and reboots the device.

Select **Device** → **Configuration** from the navigation tree, and then click the **Initialize** tab to enter the initialize confirmation page as shown in [a](#).

a. Initialize confirmation dialog box



Note: Click **Restore Factory-Default Settings** to restore and initialize the factory-default settings and reboot.

Click the **Restore Factory-Default Settings** button to restore the system to factory defaults.

Device maintenance

Software upgrade

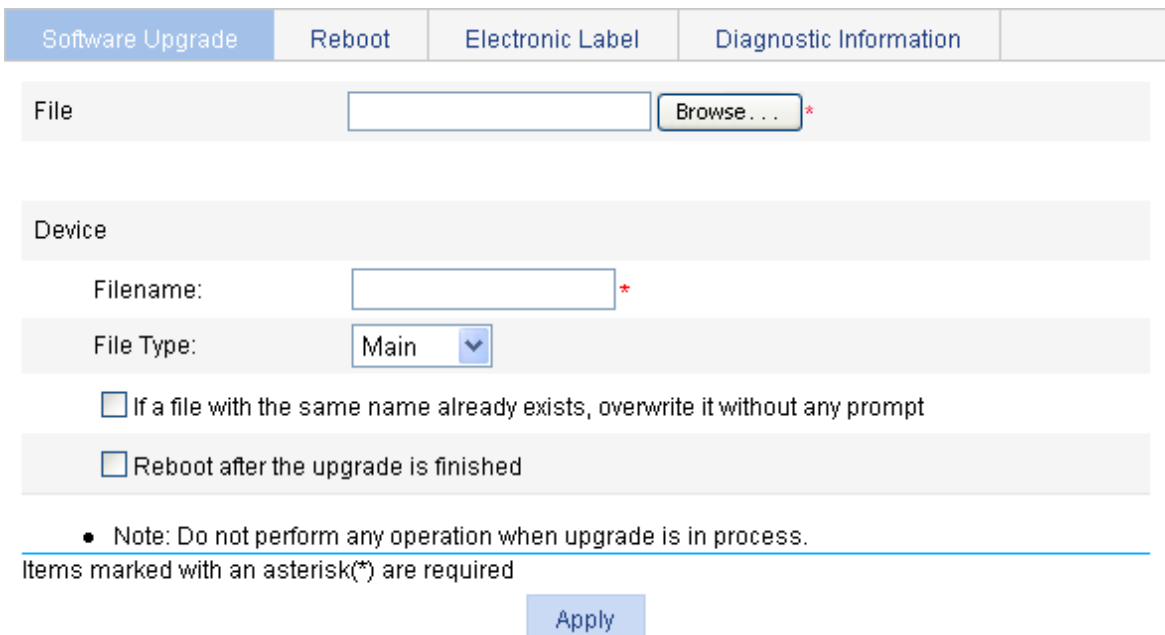
A system software image file is used to boot the device. Software upgrade allows you to obtain a target system software image file from the local host and set the file as the startup configuration file. In addition, you can select whether to reboot the device to bring the upgraded system software image file into effect.

CAUTION:

Software upgrade takes some time. Avoid performing any operation on the web interface during the upgrading procedure. Otherwise, the upgrade operation may be interrupted.

Select **Device** → **Device Maintenance** from the navigation tree to enter the software upgrade configuration page, as shown in [a](#).

a. Software upgrade configuration page



Software Upgrade | Reboot | Electronic Label | Diagnostic Information

File

Device

Filename:

File Type:

If a file with the same name already exists, overwrite it without any prompt

Reboot after the upgrade is finished

• Note: Do not perform any operation when upgrade is in process.
Items marked with an asterisk(*) are required

2. Software upgrade configuration items

Item	Description
File	Specifies the filename of the local system software image file, which must be with an extension .bin .
Filename	Specifies a filename for the file to be saved on the device. The filename must have an extension, which must be the same as that of the source file.

Item	Description
File Type	Specifies the type of the startup configuration file: <ul style="list-style-type: none"> • Main • Backup
If a file with same name already exists, overwrite it without prompt.	Specifies whether to overwrite the file with the same name. If you do not select the option, when a file with the same name exists, a dialog box appears, telling you that the file already exists and you cannot continue the upgrade.
Reboot after the upgrading finished.	Specifies whether to reboot the device to make the upgraded system software image file take effect after the system software image file is uploaded.

Device reboot

⚠ CAUTION:

- Before rebooting the device, save the configuration; otherwise, all unsaved configuration will be lost after device reboot.
- When the device reboots, you need to re-log in to the web interface.

Select **Device** → **Device Maintenance** from the navigation tree, click the **Reboot** tab to enter the device reboot configuration page, as shown in a.

a. Device reboot page

Software Upgrade	Reboot	Electronic Label	Diagnostic Information
------------------	---------------	------------------	------------------------

Device Reboot

Any configuration changes that have not been saved will be lost when the system reboots.

Check whether the current configuration is saved in the next startup configuration file.

Apply

Click **Apply** to reboot the device. You can check whether the current configuration has been saved to the startup configuration file.

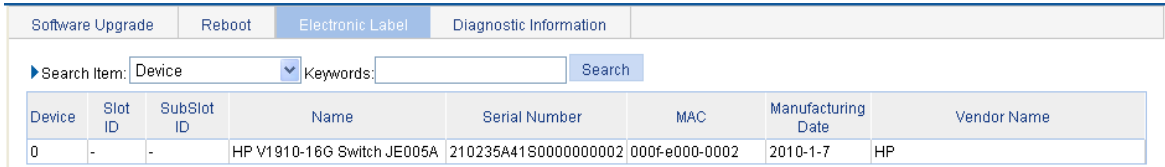
- If you select **Check configuration with next startup configuration file**, the system checks the configuration before rebooting the device. If the check succeeds, the system reboots the device; if the check fails, a dialog box appears, telling you that the current configuration and the saved configuration are inconsistent, and the device will not be rebooted. In this case, you need to save the current configuration manually before you can reboot the device.
- If you do not select the check box, the system reboots the device directly.

Electronic label

Electronic label allows you to view information about the device electronic label, which is also known as the permanent configuration data or archive information. The information is written into the storage medium of a device or a card during the debugging and testing processes, and includes the card name, product bar code, MAC address, debugging and testing date(s), manufacture name, and so on.

Select **Device** → **Device Maintenance** from the navigation tree, and click the **Electronic Label** tab to enter the page as shown in [a](#).

a. Electronic label



Device	Slot ID	SubSlot ID	Name	Serial Number	MAC	Manufacturing Date	Vendor Name
0	-	-	HP V1910-16G Switch JE005A	210235A4180000000002	000fe000-0002	2010-1-7	HP

Diagnostic information

Each functional module has its own running information, and generally, you view the output information for each module one by one. To receive as much information as possible in one operation during daily maintenance or when system failure occurs, the diagnostic information module allows you to save the running statistics of multiple functional modules to a file named **default.diag**. This allows you to locate problems faster by checking this file.

Select **Device** → **Device Maintenance** from the navigation tree, and click the **Diagnostic Information** tab to enter the page as shown in [a](#).

a. Diagnostic information



- Note: The operation may take a long time. Do not perform any operation when creating diagnostic information file is in process.

When you click **Create Diagnostic Information File**, the system begins to generate a diagnostic information file, and after the file is generated, the page is as shown in [b](#).

b. The diagnostic information file is created



[Click to Download](#)

- Note: The operation may take a long time. Do not perform any operation when creating diagnostic information file is in process.

Creating diagnostic information file succeeded.

Click **Click to Download**, and the **File Download** dialog box appears. You can select to open this file or save this file to the local host.

NOTE:

- The generation of the diagnostic file takes some time. During this process, do not perform any operation on the web page.
 - After the diagnostic file is generated successfully, you can view this file by selecting **Device** → **File Management**, or downloading this file to the local host. For more information, see the chapter “File management configuration”.
-

File management

The device saves files such as host software and configuration file into the storage device, and provides the file management function for users to manage those files conveniently and effectively. File management function provides the following operations:

- Displaying file list
- Downloading a file
- Uploading a file
- Removing a file

File management configuration

Displaying file list

Select **Device** → **File Management** from the navigation tree to enter the file management page, as shown in a. Select a disk from the **Please select disk** drop-down list on the top of the page, and the page then displays used space, free space and capacity of the disk at the right of the drop-down list, and all files saved in this disk (in the format of path + filename) and file sizes.

a. File management

File Management

Please select disk **flash** Used space: 11.56 MB Free space: 84.44 MB Capacity: 96.00 MB

<input type="checkbox"/>	File	Size(KB)	Operation
<input type="checkbox"/>	flash:/default.diag	243.858	
<input type="checkbox"/>	flash:/system.xml	0.147	
<input type="checkbox"/>	flash:/startup.cfg	1.969	
<input type="checkbox"/>	flash:/v1910-cmw520-a1108.bin	10,021.625	
<input type="checkbox"/>	flash:/aa.cfg	1.587	
<input type="checkbox"/>	flash:/logfile/logfile.log	7.395	

6 records, 15 per page | page 1/1, record 1-6 | First Prev Next Last 1 GO

[Download File](#) [Remove File](#)

Upload File

Please select disk **flash**

File [Browse...](#)

- Note: Do not perform any operation when upload is in process.

[Apply](#)

Downloading a file

Select **Device** → **File Management** from the navigation tree to enter the file management page, as shown in [a](#). Select a file from the list, click the **Download File** button, and then a **File Download** dialog box appears. You can select to open the file or to save the file locally, and you can download only one file at a time.

Uploading a file


Select **Device** → **File Management** from the navigation tree to enter the file management page, as shown in [a](#). In the **Upload File** area, select a disk from the **Please select disk** drop-down list to save the file, and then select the file path and filename by clicking **Browse**. Click **Apply** to upload the file to the specified storage device.

CAUTION:

Uploading a file takes some time. HP recommends you not to perform any operation on the web interface during the upgrading procedure.

Removing a file

Select **Device** → **File Management** from the navigation tree to enter the file management page, as shown in [a](#). You can remove a file by using one of the following ways:

- Click the  icon to remove a file.
- Select one or multiple files from the file list, and then click **Remove File**.

Port management configuration

You can use the port management feature to set and view the operation parameters of a Layer 2 Ethernet port, including but not limited to its state, rate, duplex mode, link type, PVID, MDI mode, flow control settings, MAC learning limit, and storm suppression ratios.

Configuring a port

Setting operation parameters for a port

Select **Device** → **Port Management** from the navigation tree, and then select the **Setup** tab on the page that appears to enter the page as shown in [a](#).

a. The Setup tab

Summary | Detail | **Setup**

Basic Configuration

Port State: No Change | Speed: No Change | Duplex: No Change

Link Type: No Change | PVID: (1-4094)

Advanced Configuration

MDI: No Change | Flow Control: No Change

Power Save: No Change | Max MAC Count: No Change (0-8192)

Storm Suppression

Broadcast Suppression: No Change | Multicast Suppression: No Change | Unicast Suppression: No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kpbs range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

HP V1910-16G Sw...

Select All | Select None

Unit	Selected Ports
1	

• It may take some time if you apply the above settings to multiple ports. Apply Cancel

2. Port configuration items

Item	Description
Port State	Enable or disable the port. Sometimes, after you modify the operation parameters of a port, you need to disable and then enable the port to have the modifications take effect.
Speed	<p>Set the transmission rate of the port.</p> <p>Available options include:</p> <ul style="list-style-type: none">• 10: 10 Mbps• 100: 100 Mbps• 1000: 1000 Mbps• Auto: auto-negotiation• Auto 10: auto-negotiated to 10 Mbps• Auto 100: auto-negotiated to 100 Mbps• Auto 1000: auto-negotiated to 1000 Mbps• Auto 10 100: auto-negotiated to 10 or 100 Mbps• Auto 10 1000: auto-negotiated to 10 or 1000 Mbps• Auto 100 1000: auto-negotiated to 100 or 1000 Mbps• Auto 10 100 1000: auto-negotiated to 10, 100, or 1000 Mbps <p>⚠ IMPORTANT: SFP optical ports do not support the 10 or 100 option.</p>
Duplex	<p>Set the duplex mode of the port.</p> <ul style="list-style-type: none">• Auto: auto-negotiation• Full: full duplex• Half: half duplex <p>⚠ IMPORTANT: Ethernet electrical ports whose transmission rate is configured as 1000 Mbps and SFP optical ports do not support the half option.</p>
Link Type	<p>Set the link type of the current port, which can be access, hybrid, or trunk. For more information, see the chapter “VLAN configuration.”</p> <p>⚠ IMPORTANT: To change the link type of a port from trunk to hybrid or vice versa, you must first set its link type to access.</p>
PVID	<p>Set the default VLAN ID of the interface. For more information about setting the PVID, see the chapter “VLAN configuration.”</p> <p>⚠ IMPORTANT: To enable a link to properly transmit packets, be sure the trunk or hybrid ports at the two ends of the link have the same PVID.</p>

Item	Description
MDI	<p>Set the Medium Dependent Interface (MDI) mode of the port. Two types of Ethernet cables can be used to connect Ethernet devices: crossover cable and straight-through cable. To accommodate these two types of cables, an Ethernet port can operate in one of the following three MDI modes: across, normal, and auto.</p> <p>An Ethernet port is composed of eight pins. By default, each pin has its particular role. For example, pin 1 and pin 2 are used for transmitting signals; pin 3 and pin 6 are used for receiving signals. You can change the pin roles by setting the MDI mode.</p> <ul style="list-style-type: none"> • For an Ethernet port in across mode, pin 1 and pin 2 are used for transmitting signals; pin 3 and pin 6 are used for receiving signals. The pin roles are cannot be changed. • For an Ethernet port in auto mode, the pin roles are decided through auto negotiation. • For an Ethernet port in normal mode, the pin roles are changed. Pin 1 and pin 2 are used for receiving signals; pin 3 and pin 6 are used for transmitting signals. <p>To enable normal communication, you must connect the local transmit pins to the remote receive pins. Therefore, you should configure the MDI mode depending on the cable types.</p> <ul style="list-style-type: none"> • HP does not recommend you to use the auto mode. The other two modes are used only when the device cannot determine the cable type. • When straight-through cables are used, the local MDI mode must be different from the remote MDI mode. • When crossover cables are used, the local MDI mode must be the same as the remote MDI mode, or the MDI mode of at least one end must be set to auto. <p>! IMPORTANT: SFP optical ports do not support this feature.</p>
Flow Control	<p>Enable or disable flow control on the port.</p> <p>With flow control enabled at both sides, when traffic congestion occurs on the ingress port, the ingress port will send a Pause frame notifying the egress port to temporarily suspend the sending of packets. The egress port is expected to stop sending any new packet when it receives the Pause frame. In this way, flow control helps to avoid dropping of packets.</p> <p>! IMPORTANT: Flow control works only after it is enabled on both the ingress and egress ports.</p>
Power Save	<p>Enable or disable auto power down on the port.</p> <p>With auto power down enabled, when an Ethernet port does not receive any packet for a certain period of time, it automatically enters the power save mode and resumes its normal state upon the arrival of a packet.</p> <p>By default, auto power down is disabled.</p>
Max MAC Count	<p>Set the MAC learning limit on the port. Available options include:</p> <ul style="list-style-type: none"> • User Defined: Select this option to set the limit manually. • No Limited: Select this option to set no limit.

Item	Description
Broadcast Suppression	<p>Set broadcast suppression on the port. You can suppress broadcast traffic by percentage or by PPS as follows:</p> <ul style="list-style-type: none"> ratio: Sets the maximum percentage of broadcast traffic to the total bandwidth of an Ethernet port. When this option is selected, you need to input a percentage in the box below. pps: Sets the maximum number of broadcast packets that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. kbps: Sets the maximum number of broadcast kilobits that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. <p>! IMPORTANT:</p> <p>Do not configure this item if the storm constrain function for broadcast traffic is enabled on the port. Otherwise, the suppression result will be unpredictable. To set storm constrain for broadcast traffic on a port, select Device → Storm Constrain.</p>
Multicast Suppression	<p>Set multicast suppression on the port. You can suppress multicast traffic by percentage or by PPS as follows:</p> <ul style="list-style-type: none"> ratio: Sets the maximum percentage of multicast traffic to the total bandwidth of an Ethernet port. When this option is selected, you need to input a percentage in the box below. pps: Sets the maximum number of multicast packets that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. kbps: Sets the maximum number of multicast kilobits that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. <p>! IMPORTANT:</p> <p>Do not configure this item if the storm constrain function for multicast traffic is enabled on the port. Otherwise, the suppression result will be unpredictable. To set storm constrain for multicast traffic on a port, select Device → Storm Constrain.</p>
Unicast Suppression	<p>Set unicast suppression on the port. You can suppress unicast traffic by percentage or by PPS as follows:</p> <ul style="list-style-type: none"> ratio: Sets the maximum percentage of unicast traffic to the total bandwidth of an Ethernet port. When this option is selected, you need to input a percentage in the box below. pps: Sets the maximum number of unicast packets that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. kbps: Sets the maximum number of unicast kilobits that can be forwarded on an Ethernet port per second. When this option is selected, you need to input a number in the box below. <p>! IMPORTANT:</p> <p>Do not configure this item if the storm constrain function for unicast traffic is enabled on the port. Otherwise, the suppression result will be unpredictable. To set storm constrain for unicast traffic on a port, select Device → Storm Constrain.</p>

Item	Description
Selected Ports	<p>Port or ports that you have selected from the chassis front panel and the aggregate interface list below, for which you have set operation parameters.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> Only in the presence of link aggregations groups, Aggregation ports will be displayed under the chassis front panel. You can set only the state and MAC learning limit for an aggregate interface.

Viewing the operation parameters of a port

Select **Device** → **Port Management** from the navigation tree. The **Summary** tab is displayed by default. Select the parameter you want to view by clicking the radio button before it to display the setting of this parameter for all the ports in the lower part of the page, as shown in **a**.

a. The Summary tab

Select Feature:

PortState Max MAC Count
 Flow Control Default VLAN ID(PVID)
 Link Type MDI
 Duplex Speed
 Broadcast Suppression
 Multicast Suppression Unicast Suppression
 Power Save

Feature Summary:

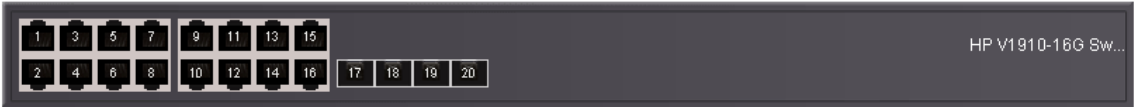
Ports	Setting
GE1/0/1	Enabled
GE1/0/2	Enabled
GE1/0/3	Enabled
GE1/0/4	Enabled
GE1/0/5	Enabled
GE1/0/6	Enabled
GE1/0/7	Enabled
GE1/0/8	Enabled

Select **Device** → **Port Management** from the navigation tree, select the **Details** tab on the page that appears, and then click the port whose operation parameters you want to view in the chassis front panel, as shown in **b**. The operation parameter settings of the selected port are displayed on the lower part of the page (in the square brackets).

b. The Details tab

Summary **Detail** Setup

Select a Port



Port State	PVID
Flow Control	Link Type
MDI	Speed
Duplex	Max MAC Count
Broadcast Suppression	
Multicast Suppression	Unicast Suppression
Power Save	

The table shows the configured values for the selected port, while those inside the square brackets are the actual values of the selected port.

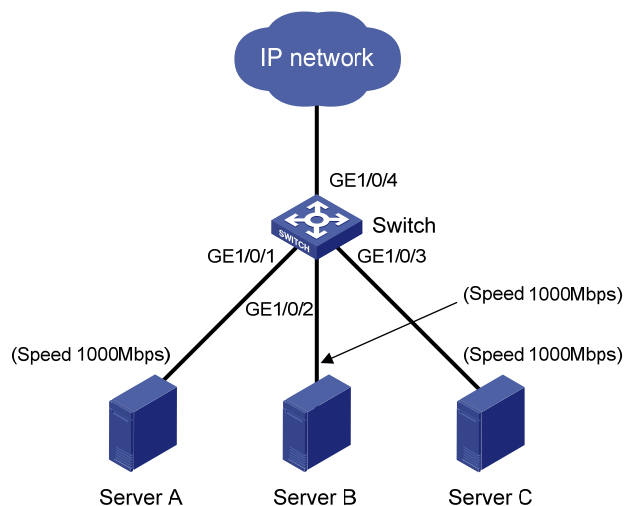
Port management configuration example

Network requirements

As shown in a:

- Server A, Server B, and Server C are connected to GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 or the switch respectively. The rates of the network adapters of these servers are all 1000 Mbps.
- The switch connects to the external network through GigabitEthernet 1/0/4 whose rate is 1000 Mbps.
- To avoid congestion at the egress port, GigabitEthernet 1/0/4, configure the auto-negotiation rate range on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 as 100 Mbps.

a. Network diagram for port rate configuration



Configuration procedure

Set the rate of GigabitEthernet 1/0/4 to 1000 Mbps.

- Select **Device** → **Port Management** from the navigation tree, click the **Setup** tab to enter the page shown in a, and make the following configurations:

a. Configure the rate of GigabitEthernet 1/0/4

Summary Detail **Setup**

Basic Configuration

Port State: No Change ▾ Speed: 1000 ▾ Duplex: No Change ▾

Link Type: No Change ▾ PVID: (1-4094)

Advanced Configuration

MDI: No Change ▾ Flow Control: No Change ▾

Power Save: No Change ▾ Max MAC Count: No Change ▾ (0-8192)

Storm Suppression

Broadcast Suppression: No Change ▾ Multicast Suppression: No Change ▾ Unicast Suppression: No Change ▾

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kpbs range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

HP V1910-16G Sw...

Select All Select None

Unit	Selected Ports
1	GE1/0/4

• It may take some time if you apply the above settings to multiple ports. **Apply** **Cancel**

- Select **1000** in the **Speed** dropdown list.
- Select GigabitEthernet 1/0/4 on the chassis front panel.
- Click **Apply**.

Batch configure the auto-negotiation rate range on GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 as 100 Mbps.

- Select **Auto 100** in the **Speed** dropdown list on the page shown in b.
- Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.
- Click **Apply**.

b. Batch configure port rate

Summary Detail **Setup**

Basic Configuration

Port State Speed Duplex

Link Type PVID (1-4094)

Advanced Configuration

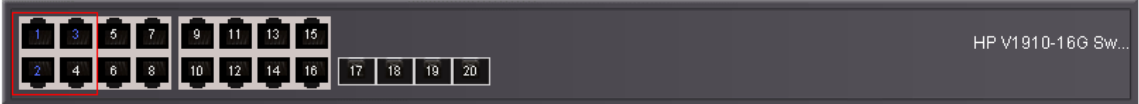
MDI Flow Control

Power Save Max MAC Count (0-8192)

Storm Suppression

Broadcast Suppression Multicast Suppression Unicast Suppression

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kpps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)



Unit	Selected Ports
1	GE1/0/1-GE1/0/3

- It may take some time if you apply the above settings to multiple ports.

Display the rate settings of ports.

- Click the **Summary** tab.
- Select the **Speed** option to display the rate information of all ports on the lower part of the page, as shown in [c](#).

c. Display the rate settings of ports

Summary	Detail	Setup
---------	--------	-------

Select Feature:

- PortState
- Flow Control
- Link Type
- Duplex
- Broadcast Suppression
- Multicast Suppression
- Power Save
- Max MAC Count
- Default VLAN ID(PVID)
- MDI
- Speed
- Unicast Suppression

Feature Summary:

Ports	Setting
GE1/0/1	Auto (100M)
GE1/0/2	Auto (100M)
GE1/0/3	Auto (100M)
GE1/0/4	1000M
GE1/0/5	Auto
GE1/0/6	Auto
GE1/0/7	Auto
GE1/0/8	Auto

Port mirroring configuration

Introduction to port mirroring

Port mirroring is the process of copying the packets passing through a port (called a mirroring port) to another port (called the monitor port) connected with a monitoring device for packet analysis.

You can mirror inbound, outbound, or bidirectional traffic on a port as needed.

Implementing port mirroring

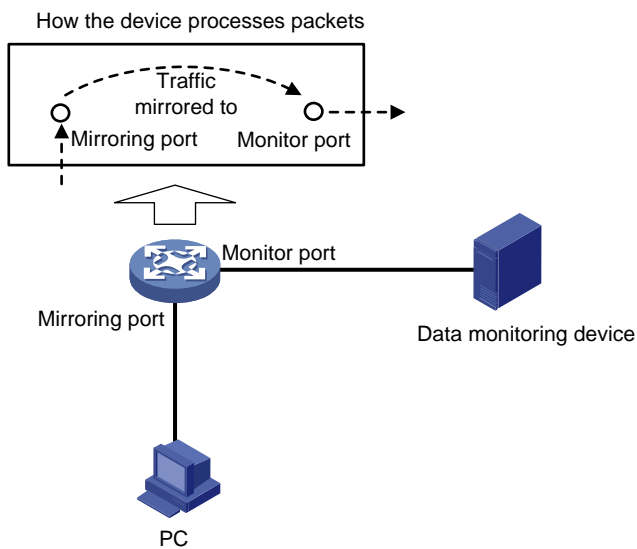
Port mirroring is implemented through local port mirroring groups. The following subsections describe how local port mirroring is implemented.

Local port mirroring

In local port mirroring, all packets (including protocol and data packets) passing through a port can be mirrored. Local port mirroring is implemented through a local mirroring group.

As shown in a, packets on the mirroring port are mirrored to the monitor port for the data monitoring device to analyze.

a. Local port mirroring implementation



Configuring local port mirroring

Configuration task list

Configuring local port mirroring

To configure local port mirroring, you must create a local mirroring group and then specify the mirroring ports and monitor port for the group.

1. Local port mirroring configuration task list

Task	Remarks
Create a local mirroring group	Required For more information, see “Creating a mirroring group” .
Configure the mirroring ports	Required For more information, see “Configuring ports for a mirroring group” . During configuration, you need to select the port type Mirror Port . You can configure multiple mirroring ports for a mirroring group.
Configure the monitor port	Required For more information, see “Configuring ports for a mirroring group” . During configuration, you need to select the port type Monitor Port . You can configure one only monitor port for a mirroring group.

Creating a mirroring group

Select **Device** → **Port Mirroring** from the navigation tree and click **Create** to enter the page for creating a mirroring group, as shown in [a](#).

a. Create a mirroring group

Summary	Create	Remove	Modify Port	
---------	--------	--------	-------------	--

Mirroring Group ID (1-1)

Type

Group ID	Type
----------	------

2. Configuration items of creating a mirroring group

Item	Description
Mirroring Group ID	ID of the mirroring group to be created
Type	Specify the type of the mirroring group to be created: <ul style="list-style-type: none">• Local: Creates a local mirroring group.

Return to [Local port mirroring configuration task list](#).

Configuring ports for a mirroring group

Select **Device** → **Port Mirroring** from the navigation tree and click **Modify Port** to enter the page for configuring ports for a mirroring group, as shown in [a](#).

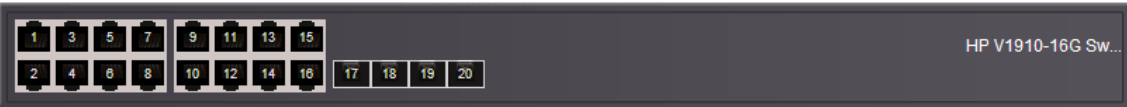
a. The Modify Port tab

Summary
Create
Remove
Modify Port

Mirroring Group ID Select Group ID

Port Type Monitor Port
Stream Orientation both

Select port(s)



Select All
Select None

Selected Port(s)

Not Available for Selection

Apply

Selected Port(s)

Note:

1. Selected Port(s): Configured member port(s).
2. Not Available for Selection: All the member ports of mirroring group on the device except Selected Port(s).

2. Configuration items of configuring ports for a mirroring group

Item	Description
Mirroring Group ID	ID of the mirroring group to be configured The available groups were created previously.
Port Type	Set the type of the port to be configured <ul style="list-style-type: none"> Configure ports for a local mirroring group: Monitor Port: Configures the monitor ports for the local mirroring group. Mirror Port: Configures mirroring ports for the local mirroring group.
Stream Orientation	Set the direction of the traffic monitored by the monitor port of the mirroring group This configuration item is available when Mirror Port is selected is the Port Type drop-down list. <ul style="list-style-type: none"> both: Mirrors both received and sent packets on mirroring ports. inbound: Mirrors only packets received by mirroring port. outbound: Mirrors only packets sent by mirroring ports.
Select port(s)	Click the ports to be configured on the chassis front panel. If aggregate interfaces are configured on the device, the page displays a list of aggregate interfaces below the chassis front panel. You can select aggregate interfaces from this list and configure them as mirroring ports of a port mirroring group.

Return to [Local port mirroring configuration task list](#).

Configuration examples

Local port mirroring configuration example

Network requirements

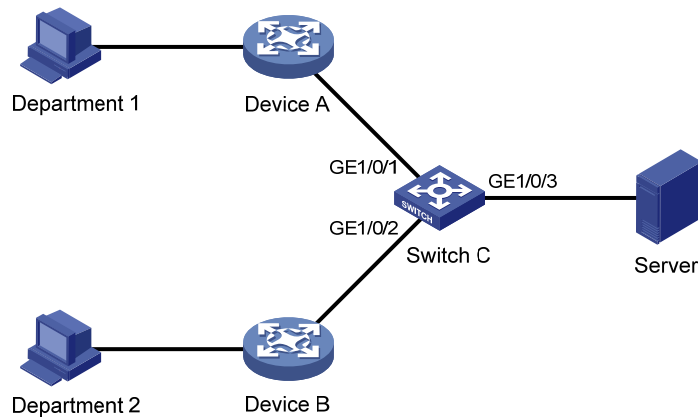
- Department 1 accesses Switch C through GigabitEthernet 1/0/1.
- Department 2 accesses Switch C through GigabitEthernet 1/0/2.
- Server is connected to GigabitEthernet 1/0/3 of Switch C.

Configure port mirroring to monitor the bidirectional traffic of Department 1 and Department 2 on the server.

To satisfy the requirement through local port mirroring, perform the following configuration on Switch C:

- Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as mirroring ports.
- Configure GigabitEthernet 1/0/3 as the monitor port.

a. Network diagram for local port mirroring configuration



Configuration procedure

Create a local mirroring group.

Select **Device** → **Port Mirroring** from the navigation tree and click **Create** to enter the page to create a local mirroring group, as shown in [a](#).

a. Create a local mirroring group

Summary	Create	Remove	Modify Port	
Mirroring Group ID	<input type="text" value="1"/>	(1-1)		
Type	<input type="text" value="Local"/>			
<input type="button" value="Apply"/>				

Group ID	Type
----------	------

- Type in mirroring group ID **1**.
- Select **Local** in the **Type** drop-down list.
- Click **Apply**.

Configure the mirroring ports.

Click **Modify Port** to enter the page for configuring the mirroring group ports, as shown in **b**.

b. Configure the mirroring ports

Summary Create Remove **Modify Port**

Mirroring Group ID **1 - Local**

Port Type **Mirror Port** Stream Orientation **both**

Select port(s)

HP V1910-16G Sw...

Select All Select None

Selected Port(s)

Not Available for Selection

Apply

Selected Port(s)

GE1/0/1-GE1/0/2

Note:

1. Selected Port(s): Configured member port(s).
2. Not Available for Selection: All the member ports of mirroring group on the device except Selected Port(s).

- Select **1 – Local** in the **Mirroring Group ID** drop-down list.
- Select **Mirror Port** in the **Port Type** drop-down list.
- Select **both** in the **Stream Orientation** drop-down list.
- Select GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on the chassis front panel.
- Click **Apply**. A configuration progress dialog box appears, as shown in c.

c. Configuration progress dialog box

Current Configuration

Add port GigabitEthernet1/0/1 - OK!

Add port GigabitEthernet1/0/2 - OK!

100%

Pause Close

- After the configuration process is complete, click **Close**.

Configure the monitor port.

Click **Modify Port** to enter the page for configuring the mirroring group ports, as shown in d.

d. Configure the monitor port

Summary Create Remove **Modify Port**

Mirroring Group ID 1 - Local

Port Type Monitor Port Stream Orientation both

Select port(s)

HP V1910-16G Sw...

Select All Select None

Selected Port(s) Not Available for Selection

Apply

Selected Port(s)
GE1/0/3

Note:

1. Selected Port(s): Configured member port(s).
2. Not Available for Selection: All the member ports of mirroring group on the device except Selected Port(s).

- Select **1 – Local** in the **Mirroring Group ID** drop-down list.
- Select **Monitor Port** in the **Port Type** drop-down list.
- Select GigabitEthernet 1/0/3 on the chassis front panel.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close** in the dialog box.

Configuration guidelines

Consider the following points during local port mirroring configuration:

- To ensure operation of your device, do not enable STP, MSTP, or RSTP on the monitor port.
- You can configure multiple mirroring ports but only one monitor port for a local mirroring group.

User management

Overview

The switch provides the following user management functions:

- Add local user accounts for FTP and Telnet users, and specify the password, access level, and service types for each user.
- Set the super password for non-management level users to switch to the management level.
- Switch to the management level from a lower level.

Managing users

Adding a local user

Select **Device** → **Users** from the navigation tree, and click the **Create** tab to add a local user, as shown in [a](#).

a. Add a user

" data-bbox="161 460 860 741"/>

Item	Description
Username	Set a username for the user

2. Local user configuration items

Item	Description
Username	Set a username for the user

Item	Description
Access Level	<p>Select an access level for the user.</p> <p>Users of different levels can perform different operations. User levels, in order from low to high, are visitor, monitor, configure, and management.</p> <ul style="list-style-type: none"> • Visitor: Users of this level can only perform ping and traceroute operations. They can neither access data on the switch nor configure the switch. • Monitor: Users of this level can perform ping and traceroute operations and access data on the switch but cannot configure the switch. • Configure: Users of this level can perform ping and traceroute operations, access data on the switch, and configure the switch, but they cannot upgrade the host software, add/delete/modify users, or back up/restore the configuration file. • Management: Users of this level can perform any operations on the switch.
Password	Set the password for the user.
Confirm Password	Input the same password again. Otherwise, the system will prompt that the two passwords are not consistent when you apply the configuration.
Password Display Mode	<p>Set the password displaying mode.</p> <p>Options include:</p> <ul style="list-style-type: none"> • Simple: Saves the password in the configuration file in plain text so that the password is displayed in plain text. • Cipher: Saves the password in the configuration file in cipher text so that the password is displayed in cipher text. <p>A plaintext password is not safe. It is good practice to use the cipher mode.</p>
Service Type	Set the service type, including FTP and Telnet services. You must select either of them.

Setting the super password

A management level user can set the password for non-management level users to switch to the management level. If the super password is not configured, no switchover can occur.

Select **Device** → **Users** from the navigation tree, and click the **Super Password** tab to set the super password.

a. Super password

Summary	Super Password	Create	Modify	Remove	Switch To Management
Please specify the super password					
<input checked="" type="radio"/> Create		<input type="radio"/> Remove			
Password	<input type="text"/>	(1-16 Chars.)			
Confirm Password	<input type="text"/>				
Password Display Mode	Simple	▼			
<input type="button" value="Apply"/>					

Note: Use the super password to switch from the current user level to the management level.

2. Super password configuration items

Item	Description
Create/Remove	Select the operation type. Options include: <ul style="list-style-type: none">• Create: Configure or modify the super password.• Remove: Remove the current super password.
Password	Set the password for non-management level users to switch to the management level.
Confirm Password	Input the same password again. Otherwise, the system will warn that the two passwords input are not consistent when you apply the configuration.
Password Display Mode	Set the password displaying mode. Options include: <ul style="list-style-type: none">• Simple: Saves the password in the configuration file in plain text so that the password is displayed in plain text.• Cipher: Saves the password in the configuration file in cipher text so that the password is displayed in cipher text. <p>A plaintext password is not safe. It is good practice to use the cipher mode.</p>

Switching to the management level

This function allows a user to switch from the current user level to the management level. To switch to the management level, a user must provide the correct super password.

The access level switchover of a user is valid for the current login only; it does not change the access level configured for the user. When the user re-logs in to the Web interface, the access level of the user is still the original level.

To switch to the management level, select **Device** → **Users** from the navigation tree, click the **Switch To Management** tab, input the correct super password, and click **Login**.

a. Switch to the management level.

Summary	Super Password	Create	Modify	Remove	Switch To Management
---------	----------------	--------	--------	--------	----------------------

Please enter the super password to switch from the current user level to the management level.

Password (1-16 Chars.)

Login

Loopback test configuration

Overview

You can check whether an Ethernet port works normally by performing the Ethernet port loopback test, during which the port cannot forward data packets normally.

Ethernet port loopback test can be an internal loopback test or an external loopback test.

- In an internal loopback test, self loop is established in the switching chip to check whether there is a chip failure related to the functions of the port.
- In an external loopback test, a loopback plug is used on the port. Packets forwarded by the port will be received by itself through the loopback plug. The external loopback test can be used to check whether there is a hardware failure on the port.

Loopback operation

Select **Device** → **Loopback** from the navigation tree to enter the loopback test configuration page, as shown in a.

a. Loopback test configuration page

Loopback

Testing type: External Internal

HP V1910-16G Sw...

Test

Result :

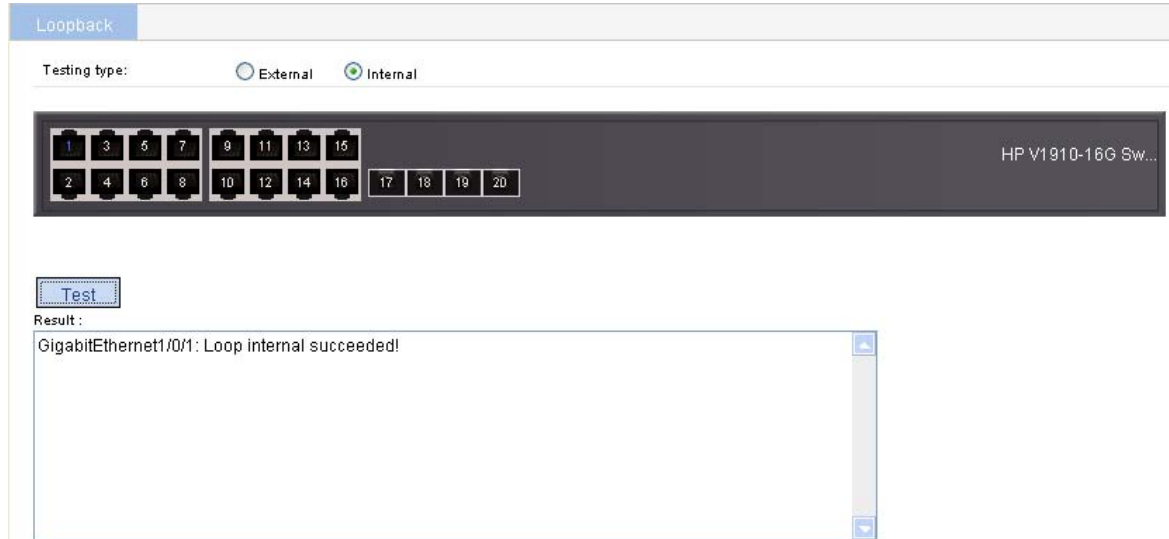
2. Loopback test configuration items

Item	Description
Testing type	External Internal
	Set the loopback test type, which can be External or Internal .

After selecting a testing type, you need to select a port on which you want to perform the loopback test from the chassis front panel.

After that, click **Test** to start the loopback test, and you can see the test result in the **Result** box, as shown in a.

a. Loopback test result



Configuration guidelines

Note the following when performing a loopback test:

- You can perform an internal loopback test but not an external loopback test on a port that is physically down, but you can perform neither test on a port that is manually shut down.
- The system does not allow **Rate**, **Duplex**, **Cable Type** and **Port Status** configuration on a port under a loopback test.
- An Ethernet port works in full duplex mode when the loopback test is performed, and restores its original duplex mode after the loopback test.

VCT

Overview

NOTE:

The fiber interface of a SFP port does not support this feature.

A link in the up state goes down and then up automatically if you perform this operation on one of the Ethernet interfaces forming the link.

You can use the Virtual Cable Test (VCT) function to check the status of the cable connected to an Ethernet port on the device. The check result is returned in less than 5 seconds. The test covers whether short circuit or open circuit occurs on the cable and the length of the faulty cable.

Testing cable status

Select **Device** → **VCT** from the navigation tree to enter the page for testing cable status. Select the port you want to test in the chassis front panel and then click **Test**. The test result is returned in less than 5 seconds and displayed in the **Result** text box, as shown in [a](#).

a. Test the status of the cable connected to an Ethernet port



VCT

HP V1910-16G Sw...


Test

Result :

GigabitEthernet1/0/3:
Cable status: abnormal(open), 0 metres
Pair Impedance mismatch: no
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db

Note: The error of the length detected is ± 5 meters.

2. Description on the cable test result

Item	Description
Cable status	<p>Status and length of the cable.</p> <p>The status of a cable can be normal, abnormal, abnormal(open), abnormal(short), or failure.</p> <ul style="list-style-type: none">• When a cable is normal, the cable length displayed is the total length of the cable.• When a cable is not normal, the cable length displayed is the length of the cable between the current port and the location where fault occurs. <p> IMPORTANT:</p> <p>The error of the length detected is within 5 meters.</p>

Flow interval configuration

Overview

With the flow interval module, you can view the number of packets and bytes sent/received by a port over the specified interval.

Monitoring port traffic statistics

Setting the traffic statistics generating interval

Select **Device** → **Flow interval** from the navigation bar, and click the **Interval Configuration** tab to enter the page shown in a.

a. The page for setting the traffic statistics generating interval

The screenshot shows the 'Interval Configuration' tab in a web interface. At the top, there are two tabs: 'Port Traffic Statistics' and 'Interval Configuration'. Below the tabs, there is a label 'Interval for generating traffic statistics:' followed by a text input field containing '300' and a tooltip that says '(5-300, it must be a multiple of 5, Default = 300)'. Below this is a 'Select ports' section with a grid of 20 port buttons (1-20) and a device name 'HP V1910-16G Sw...'. There are 'Select All' and 'Select None' buttons below the grid. Below the grid is a 'Selected Ports' text area and an 'Apply' button.

2. Traffic statistics generating interval configuration items

Item	Remarks
Interval for generating traffic statistics	Set the interval for generating port traffic statistics.
Select ports	Select ports from the chassis front panel to apply the interval to them.

Viewing port traffic statistics

Select **Device** → **Flow interval** from the navigation tree to enter the **Port Traffic Statistics** tab shown in a. On the tab, you can view the number of packets and bytes sent/received by each port over the last interval.

a. Port traffic statistics

Port Traffic Statistics		Interval Configuration			
▶ Search Item: <input type="text" value="Interface Name"/> Keywords: <input type="text"/>		<input type="button" value="Search"/>			
Interface Name	Interval (Sec)	Received Packet (packet/Sec)	Sent Packet (packet/Sec)	Received Byte (byte/Sec)	Sent Byte (byte/Sec)
GigabitEthernet1/0/16	300	0	0	0	0
GigabitEthernet1/0/17	300	0	0	0	0
GigabitEthernet1/0/18	300	0	0	0	0
GigabitEthernet1/0/19	300	0	0	0	0
GigabitEthernet1/0/20	300	0	0	0	0
GigabitEthernet1/0/21	300	0	0	0	0
GigabitEthernet1/0/22	300	0	0	0	0
GigabitEthernet1/0/23	300	0	0	0	0
GigabitEthernet1/0/24	300	3	2	657	2409
GigabitEthernet1/0/25	300	0	0	0	0
GigabitEthernet1/0/26	300	0	0	0	0
GigabitEthernet1/0/27	300	0	0	0	0
GigabitEthernet1/0/28	300	0	0	0	0

28 records, per page | page 2/2, record 16-28 | [First](#) [Prev](#) [Next](#) [Last](#)

Storm constrain configuration

Overview

The storm constrain function limits traffic of a port within a predefined upper threshold to suppress packet storms in an Ethernet. With this function enabled on a port, the system detects the amount of broadcast traffic, multicast traffic, and unicast traffic reaching the port periodically. When a type of traffic exceeds the threshold for it, the function, as configured, blocks or shuts down the port, and optionally, sends trap messages and logs.

△ CAUTION:

Alternatively, you can configure the storm suppression function to control a specific type of traffic. Because the storm suppression function and the storm constrain function are mutually exclusive, do not enable them at the same time on an Ethernet port. For example, with broadcast storm suppression enabled on a port, do not enable storm constrain for broadcast traffic on the port. The storm suppression function is configured in **Device → Port Management**. For more information, see the chapter “Port management configuration”.

With storm constrain enabled on a port, you can specify the system to act as follows when a certain type of traffic (broadcast, multicast, or unicast) exceeds the corresponding upper threshold:

- **Block**—Blocks the port. The port is blocked and stops forwarding the traffic of this type until the type of traffic drops down below the lower threshold. A port blocked by the storm constrain function can still forward other types of traffic and collect statistics for the blocked traffic.
- **Shutdown**—Shuts down the port. The port is shut down and stops forwarding all types of traffic. To bring up the port, select **Device → Port Management** to configure the port, or cancel the storm constrain setting on the port.

Configuring storm constrain

Setting the traffic statistics generating interval

Select **Device → Storm Constrain** from the navigation tree to enter the page shown in [a](#). In the **Interval for generating traffic statistics** text box, input the traffic statistics generating interval for storm constrain.

a. The Storm Constrain tab

Storm Constrain

Interval Configuration

Interval for generating traffic statistics: Seconds(1-300, Default = 10)

Port Storm Constrain

▼ Search Item: Keywords:

Match case and whole word

Search in previous results

<input type="checkbox"/>	Interface Name	Broadcast Storm Control Info	Multicast Storm Control Info	Unicast Storm Control Info	Control Mode	Trap	Log	Operation
--------------------------	----------------	------------------------------	------------------------------	----------------------------	--------------	------	-----	-----------

NOTE:

The traffic statistics generating interval set here is the interval used by the storm constrain function for measuring traffic against the traffic thresholds. It is different from the interval set in the flow interval module, which is used for measuring the average traffic sending and receiving rates over a specific interval.

For network stability sake, set the traffic statistics generating interval for the storm constrain function to the default or a greater value.

Configuring storm constrain

Select **Device** → **Storm Constrain** from the navigation tree to enter the page shown in a. In the **Port Storm Constrain** area, the configured port storm constrain settings are displayed. Click **Add** to enter the page for adding port storm constrain configuration, as shown in a.

a. Add storm constrain settings for ports

Storm Constrain

Add Port Storm Constrain

Control Mode : None ▼

Broadcast Threshold : None ▼

Multicast Threshold : None ▼

Unicast Threshold : None ▼

pps range(100M:1-148810; GE:1-1488100; 10GE:1-14881000)

Trap Log

Select ports

1

3

5

7

9

11

13

15

17

18

19

20

HP V1910-16G Sw...

Select All
Select None

Selected Ports

Apply
Cancel

2. Port storm constrain configuration items

Item	Remarks
Control Mode	<p>Specify the action to be performed when a type of traffic exceeds the corresponding upper threshold. Available options include:</p> <ul style="list-style-type: none"> None—Performs no action. Block—Blocks the traffic of this type on a port when the type of traffic exceeds the upper threshold. Shutdown—Shuts down the port when a type of traffic exceeds the traffic threshold. The port stops forwarding traffic as a result. <p>! IMPORTANT:</p> <p>The storm constrain function, after being enabled, requires a full traffic statistics generating interval (in seconds) to collect traffic data, and analyzes the data in the next interval. It is normal that a period longer than one traffic statistics generating interval is waited for a control action to happen if you enable the function while the packet storm is present. Nevertheless, the action will be taken within two intervals.</p>
Broadcast Threshold	Set the broadcast, multicast, and unicast thresholds.
Multicast Threshold	<ul style="list-style-type: none"> None—Performs no storm constrain for the selected port or ports. pps—Specifies the storm constrain upper threshold and lower threshold in packets per second (pps). <p>! IMPORTANT:</p>
Unicast Threshold	<ul style="list-style-type: none"> On a port, you can set the thresholds for broadcast, multicast, and unicast traffic at the same time. To set storm constrain on a port successfully, you must specify the thresholds for at least a type of traffic. When the pps option is selected, the upper threshold and lower threshold ranges depend on the interface type, as shown in the pps range description on the page.

Item	Remarks
Trap	Select or clear the option to enable or disable the system to send trap messages both when an upper threshold is crossed and when the corresponding lower threshold is crossed after that.
Log	Select or clear the option to enable or disable the system to output logs both when an upper threshold is crossed and when the corresponding lower threshold is crossed after that.
Select ports	Select ports from the chassis front panel to apply the storm constrain settings to them.

RMON configuration

Remote Monitoring (RMON) is used for management devices to monitor and manage the managed devices on the network by implementing such functions as statistics collection and alarm generation. The statistics collection function enables a managed device to periodically or continuously track various traffic information on the network segments connecting to its ports, such as total number of received packets or total number of oversize packets received. The alarm function enables a managed device to monitor the value of a specified MIB variable, log the event and send a trap to the management device when the value reaches the threshold, such as the port rate reaches a certain value or the portion of broadcast packets received in the total packets reaches a certain value.

Both the RMON protocol and the Simple Network Management Protocol (SNMP) are used for remote network management:

- RMON is implemented on the basis of the SNMP, and is an enhancement to SNMP. RMON sends traps to the management device to notify the abnormality of the alarm variables by using the SNMP trap packet sending mechanism. Although trap is also defined in SNMP, it is usually used to notify the management device whether some functions on managed devices operate normally and the change of physical status of interfaces. Traps in RMON and those in SNMP have different monitored targets, triggering conditions, and report contents.
- RMON provides an efficient means of monitoring subnets and allows SNMP to monitor remote network devices in a more proactive, effective way. The RMON protocol defines an alarm threshold on the managed device and when that threshold is reached, the managed device sends a trap to the management device automatically. This method reduces the communication traffic between the management device and the managed device because the management device does not need to retrieve and compare the values of MIB variables multiple times. In this way, you can manage a large scale of network easily and effectively.

Working mechanism

RMON allows multiple monitors (management devices). A monitor provides the following methods for data gathering:

- Using RMON probes. Management devices can obtain management information from RMON probes directly and control network resources. In this approach, management devices can obtain all RMON MIB information.
- Embedding RMON agents in network devices such as routers, switches, and hubs to provide the RMON probe function. Management devices exchange data with RMON agents by using basic SNMP operations to gather network management information, which, due to system resources limitation, only covers four groups of MIB information alarm, event, history, and statistics, in most cases.

The HP device adopts the second way and includes the RMON agent function. With the RMON agent function, the management device can obtain the traffic flow among the managed devices on each connected network segments and obtain information about error statistics and performance statistics for network management.

RMON groups

Among the RMON groups defined by RMON specifications (RFC 2819), the device uses the statistics group, history group, event group, and alarm group supported by the public MIB. In addition, HP defines and implements a private alarm group, which enhances the functions of the alarm group. This section describes the five kinds of groups.

Ethernet statistics group

The statistics group defines the statistics that the system collects on various traffic information on a particular interface (at present, only Ethernet interfaces are supported) and saves the statistics in the Ethernet statistics table (ethernetStatsTable) for query convenience of the management device. It provides statistics about network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, packets received, and so on.

After the creation of a statistics entry on an interface, the statistics group starts to collect traffic statistics on the interface. The result of the statistics is a cumulative sum.

History group

The history group defines the statistics that the system periodically collects on traffic information at a particular interface and saves the statistics in the history record table (ethernetHistoryTable) for query convenience of the management device. The statistics includes bandwidth utilization, number of error packets, and total number of packets.

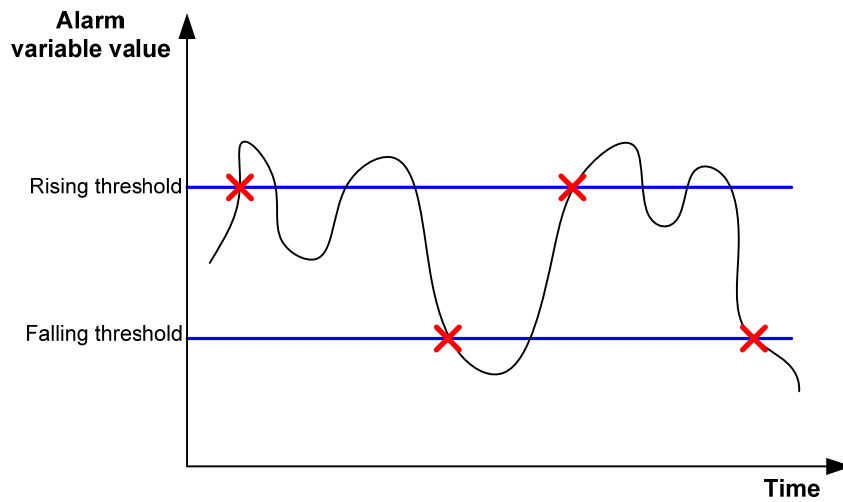
A history group collects statistics on packets received on the interface during each period, which can be configured through the command line interface (CLI).

Alarm group

The RMON alarm group monitors specified alarm variables, such as total number of received packets (etherStatsPkts) on an interface. After you define an alarm entry, the system gets the value of the monitored alarm variable at the specified interval. When the value of the monitored variable is greater than or equal to the rising threshold, a rising event is triggered; when the value of the monitored variable is smaller than or equal to the falling threshold, a falling event is triggered. The event is then handled as defined in the event group.

If the value of a sampled alarm variable surpasses the same threshold multiple times, only the first one can cause an alarm event. In other words, the rising alarm and falling alarm are alternate. As shown in [a](#), the value of an alarm variable (the black curve in the figure) surpasses the threshold value (the blue line in the figure) for multiple times, and multiple crossing points are generated, but only crossing points marked with the red crosses can trigger alarm events.

a. Rising and falling alarm events



Event group

The event group defines event indexes and controls the generation and notifications of the events triggered by the alarms defined in the alarm group and the private alarm group. The events can be handled in one of the following ways:

- Log—Logging event related information (the occurred events, contents of the event, and so on) in the event log table of the RMON MIB of the device, so the management device can check the logs through the SNMP Get operation.
- Trap—Sending a trap to notify the occurrence of this event to the network management station (NMS).
- Log-Trap—Logging event information in the event log table and sending a trap to the NMS.
- None—No action.

Configuring RMON

Configuration task list

Configuring the RMON statistics function

RMON statistics function can be implemented by either the Ethernet statistics group or the history group, but the objects of the statistics are different, and you can configure a statistics group or a history group accordingly.

- A statistics object of the Ethernet statistics group is a variable defined in the Ethernet statistics table, and the recorded content is a cumulative sum of the variable from the time the statistics entry is created to the current time. Perform the tasks in [1](#) to configure RMON Ethernet statistics function.
- A statistics object of the history group is the variable defined in the history record table, and the recorded content is a cumulative sum of the variable in each period. Perform the tasks in [2](#) to configure RMON history statistics function.

1. RMON statistics group configuration task list

Task	Remarks
Configuring a statistics entry	<p>Required</p> <p>You can create up to 100 statistics entries for a statistics table.</p> <p>After a statistics entry is created on an interface, the system collects statistics on various traffic information on the interface. It provides statistics about network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, packets received, and so on. The statistics are cleared after the device reboots.</p> <p>! IMPORTANT:</p> <p>Only one statistics entry can be created on one interface.</p>

2. RMON history group configuration task list

Task	Remarks
Configuring a history entry	<p>Required</p> <p>You can create up to 100 history entries for a history table.</p> <p>After an entry is created, the system periodically samples the number of packets received/sent on the current interface, and saves the statistics as an instance under the leaf node of the etherHistoryEntry table.</p> <p>! IMPORTANT:</p> <p>When you create an entry, if the value of the specified sampling interval is identical to that of the existing history entry, the system considers the configurations identical and the creation fails.</p>

Configuring the RMON alarm function

- To enable the managed devices to send traps to the NMS when the NMS triggers an alarm event, configure the SNMP agent as described in the chapter “SNMP configuration” before configuring the RMON alarm function.
- If the alarm variables that can be configured through the web interface are MIB variables defined in the history group or the statistics group, make sure that the RMON Ethernet statistics function or the RMON history statistics function is configured on the monitored Ethernet interface.

Perform the tasks in 1 to configure RMON alarm function.

1. RMON alarm configuration task list

Task	Remarks
Configuring an event entry	<p>Optional</p> <p>You can create up to 60 event entries for an event table.</p> <p>An event entry defines event indexes and the actions the system will take, including log the event, send a trap to the NMS, take no action, and log the event and send a trap to the NMS.</p> <p>! IMPORTANT:</p> <p>An entry cannot be created if the values of the specified alarm variable, sampling interval, sampling type, rising threshold and falling threshold are identical to those of an existing entry in the system.</p>
Configuring an alarm entry	<p>Required</p> <p>You can create up to 60 alarm entries for an alarm table.</p> <p>With an alarm entry created, the specified alarm event will be triggered when an abnormality occurs, and the alarm event defines how to deal with the abnormality.</p> <p>! IMPORTANT:</p> <p>An entry cannot be created if the values of the specified event description, owners, and actions are identical to those of an existing entry in the system.</p>

Displaying RMON running status

After you configure the RMON statistics function or the alarm function, you can view RMON running status and verify the configuration by performing tasks in 1.

1. Display RMON running status

Task	Remarks
Displaying RMON statistics information	View the interface statistics during the period from the time the statistics entry is created to the time the page is displayed. The statistics are cleared after the device reboots.
Displaying RMON history sampling information	After you have created a history control entry on an interface, the system calculates the information of the interface periodically and saves the information to the etherHistoryEntry table. You can perform this task to view the entries in this table. And the number of history sampling records that can be displayed and the history sampling interval are specified when you configure the history group.
Displaying RMON event logs	If you have configured the system to log an event after the event is triggered when you configure the event group, the event is recorded into the RMON log. You can perform this task to display the details of the log table

Configuring a statistics entry

Select **Device** → **RMON** from the navigation tree to enter the page of the **Statistics** tab, as shown in **a**. Click **Add** to enter the page for adding a statistics entry, as shown in **b**.

a. Statistics entry

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

► Search Item: Keywords:

<input type="checkbox"/>	Index	Interface Name	Owner	Status	Operation
<input type="checkbox"/>	1	GigabitEthernet1/0/1	user1	Active	

b. Add a statistics entry

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

Add a Statistic Group

Interface Name:

Owner: Chars.(1-127)

- Only one statistics group can be created on one interface.

Items marked with an asterisk(*) are required

2. Statistics entry configuration items

Item	Description
Interface Name	Select the name of the interface on which the statistics entry is created. Only one statistics entry can be created on one interface.
Owner	Set the owner of the statistics entry.

Return to [RMON statistics group configuration task list](#).

Configuring a history entry

Select **Device** → **RMON** from the navigation tree and click the **History** tab to enter the page, as shown in [a](#). Click **Add** to enter the page for adding a history entry, as shown in [b](#).

a. History entry

Statistics	History	Alarm	Event	Log					
▶ Search Item: <input type="text" value="Index"/> Keywords: <input type="text"/> <input type="button" value="Search"/>									
<input type="checkbox"/>	Index	Interface Name	Buckets Requested	Buckets Granted	Interval (Sec)	Owner	Status	Operation	
<input type="checkbox"/>	1	GigabitEthernet1/0/1	10000	10	360	user1	Active		
			<input type="button" value="Add"/>	<input type="button" value="Del Selected"/>					

b. Add a history entry

Statistics	History	Alarm	Event	Log		
Add a History Group						
Interface Name:		<input type="text" value="GigabitEthernet1/0/1"/>				
Buckets Granted:		<input type="text"/>	*(1-65535)			
Interval:		<input type="text"/>	*Seconds(5-3600)			
Owner:		<input type="text"/>	Chars.(1-127)			
Items marked with an asterisk(*) are required						
			<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>		

2. History entry configuration items

Item	Description
Interface Name	Select the name of the interface on which the history entry is created.
Buckets Granted	Set the capacity of the history record list corresponding to this history entry, namely, the maximum number of records that can be saved in the history record list. If the current number of the entries in the table has reached the maximum number, the system will delete the earliest entry to save the latest one. The statistics include total number of received packets on the current interface, total number of broadcast packets, total number of multicast packets in a sampling period, and so on.
Interval	Set the sampling period.
Owner	Set the owner of the entry.

Return to [RMON history group configuration task list](#).

Configuring an event entry

Select **Device** → **RMON** from the navigation tree and click the **Event** tab to enter the page, as shown in [a](#). Click **Add** to enter the page for adding an event entry, as shown in [b](#).

a. Event entry

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

► Search Item: Keywords:

<input type="checkbox"/>	Index	Description	Event Type	Event Last Trigger Time	Owner	Status
<input type="checkbox"/>	1	test	Log,Trap	-	user1	Active

b. Add an event entry

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

Add an Event Group

Description: Chars.(1-127)

Owner: Chars.(1-127)

Event Type: Log Trap

Items marked with an asterisk(*) are required

2. Event entry configuration items

Item	Description
Description	Set the description for the event.
Owner	Set the owner of the entry.
Event Type	Set the actions that the system will take when the event is triggered: <ul style="list-style-type: none">• Log—The system will log the event.• Trap—The system will send a trap in the community name of null. If both Log and Trap are selected, the system will log the event and send a trap. If none of them is selected, the system will take no action

Return to [RMON alarm configuration task list](#).

Configuring an alarm entry

Select **Device** → **RMON** from the navigation tree and click the **Alarm** tab to enter the page, as shown in [a](#). Click **Add** to enter the page for adding an alarm entry, as shown in [b](#).

a. Alarm entry

Statistics	History	Alarm	Event	Log
------------	---------	-------	-------	-----

▶ Search Item: Index Keywords:

<input type="checkbox"/>	Index	Interval (Sec)	Statics Item	Interface Name	Sampling Type	Current Sampling Value	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Status	Operation
<input type="checkbox"/>	1	10000	Number of Received Bytes	GigabitEthernet1/0/1	Absolute	0	100000000	100	1	1	user1	Active	

b. Add an alarm entry

Statistics	History	Alarm	Event	Log
------------	---------	-------	-------	-----

Add an Alarm Group

Alarm Variable

Statics Item:

Interface Name:

Sample Item

Interval: *Seconds(5-65535)

Sample Type:

Owner: Chars.(1-127)

Alarm

Create Default Event

Rising Threshold: *(0-2147483647) Rising Event:

Falling Threshold: *(0-2147483647) Falling Event:

- Before creating Alarm, please create Statistic and Event at first.

Items marked with an asterisk(*) are required


2. Alarm entry configuration items

Item	Description
Alarm variable	Statics Item Set the traffic statistics that will be collected and monitored. For more information, see 2 .
	Interface Name Set the name of the interface whose traffic statistics will be collected and monitored.

Item	Description	
Interval	Set the sampling interval.	
Sample Item	<p>Set the sampling type, including:</p> <ul style="list-style-type: none"> • Absolute—Absolute sampling, namely, to obtain the value of the variable when the sampling time is reached. • Delta—Delta sampling, namely, to obtain the variation value of the variable during the sampling interval when the sampling time is reached. 	
Owner	Set the owner of the alarm entry.	
Create Default Event	<p>Select whether to create a default event.</p> <p>The description of the default event is default event, the action is log-and-trap, and the owner is default owner.</p> <p>If there is no event, you can select to create the default event. And when the value of the alarm variable is higher than the alarm rising threshold or lower than the alarm falling threshold, the system will adopt the default action, that is, log-and-trap.</p>	
Alarm	Rising Threshold	Set the alarm rising threshold.
	Rising Event	<p>Set the action that the system will take when the value of the alarm variable is higher than the alarm rising threshold.</p> <p>If the Create Default Event check box is selected, this option is not configurable.</p>
	Falling Threshold	Set the alarm falling threshold.
	Falling Event	<p>Set the action that the system will take when the value of the alarm variable is lower than the alarm falling threshold.</p> <p>If the Create Default Event check box is selected, this option is not configurable.</p>

Return to [RMON alarm configuration task list](#).

Displaying RMON statistics information

Select **Device** → **RMON** from the navigation tree to enter the page of the **Statistics** tab, as shown in [a](#). Click the  icon of a statistics entry to enter the page as shown in [a](#), which displays all statistics items on the current interface.

a. RMON statistics information

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

Statistic Group Detail

Current Interface: GigabitEthernet1/0/1

Statistic Item	Statistic Value
Number of Received Bytes	21657
Number of Received Packets	307
Number of Received Broadcasting Packets	56
Number of Received Multicast Packets	34
Number of Received Packets With CRC Check Failed	0
Number of Received Packets Smaller Than 64 Bytes	0
Number of Received Packets Larger Than 1518 Bytes	0
Number of Received Packets Smaller Than 64 Bytes And FCS Check Failed	0
Number of Received Packets Larger Than 1518 Bytes And FCS Check Failed	0
Number of Network Conflicts	0
Number of Packet Discarding Events	0
Number of Received 64 Bytes Packets	235
Number of Received 65 to 127 Bytes Packets	67
Number of Received 128 to 255 Bytes Packets	4
Number of Received 256 to 511 Bytes Packets	1
Number of Received 512 to 1023 Bytes Packets	0
Number of Received 1024 to 1518 Bytes Packets	0

Back

Refresh


2. Fields of RMON statistics

Item	Description
Number of Received Bytes	Total number of octets received by the interface, corresponding to the MIB node etherStatsOctets.
Number of Received Packets	Total number of packets received by the interface, corresponding to the MIB node etherStatsPkts.
Number of Received Broadcasting Packets	Total number of broadcast packets received by the interface, corresponding to the MIB node etherStatsBroadcastPkts.
Number of Received Multicast Packets	Total number of multicast packets received by the interface, corresponding to the MIB node etherStatsMulticastPkts.

Item	Description
Number of Received Packets With CRC Check Failed	Total number of packets with CRC errors received on the interface, corresponding to the MIB node etherStatsCRCAAlignErrors.
Number of Received Packets Smaller Than 64 Bytes	Total number of undersize packets (shorter than 64 octets) received by the interface, corresponding to the MIB node etherStatsUndersizePkts.
Number of Received Packets Larger Than 1518 Bytes	Total number of oversize packets (longer than 1518 octets) received by the interface, corresponding to the MIB node etherStatsOversizePkts.
Number of Received Packets Smaller Than 64 Bytes And FCS Check Failed	Total number of undersize packets (shorter than 64 octets) with CRC errors received by the interface, corresponding to the MIB node etherStatsFragments.
Number of Received Packets Larger Than 1518 Bytes And FCS Check Failed	Number of oversize packets (longer than 1518 octets) with CRC errors received by the interface, corresponding to the MIB node etherStatsJabbers.
Number of Network Conflicts	Total number of collisions received on the interface, corresponding to the MIB node etherStatsCollisions.
Number of Packet Discarding Events	Total number of drop events received on the interface, corresponding to the MIB node etherStatsDropEvents.
Number of Received 64 Bytes Packets	Total number of received packets with 64 octets on the interface, corresponding to the MIB node etherStatsPkts64Octets.
Number of Received 65 to 127 Bytes Packets	Total number of received packets with 65 to 127 octets on the interface, corresponding to the MIB node etherStatsPkts65to127Octets.
Number of Received 128 to 255 Bytes Packets	Total number of received packets with 128 to 255 octets on the interface, corresponding to the MIB node etherStatsPkts128to255Octets.
Number of Received 256 to 511 Bytes Packets	Total number of received packets with 256 to 511 octets on the interface, corresponding to the MIB node etherStatsPkts256to511Octets.
Number of Received 512 to 1023 Bytes Packets	Total number of received packets with 512 to 1023 octets on the interface, corresponding to the MIB node etherStatsPkts512to1023Octets.
Number of Received 1024 to 1518 Bytes Packets	Total number of received packets with 1024 to 1518 octets on the interface, corresponding to the MIB node etherStatsPkts1024to1518Octets.

Return to [Display RMON running status](#).

Displaying RMON history sampling information

Select **Device** → **RMON** from the navigation tree and click the **History** tab to enter the page, as shown in [a](#). Click the  icon of a history entry to enter the page as shown in [a](#), which displays all history sampling information on the current interface.

a. RMON history sampling information

Statistics	History	Alarm	Event	Log									
History Group Detail													
Current Interface: GigabitEthernet1/0/1													
▶ Search Item: Time <input type="text"/> Keywords: <input type="text"/> <input type="button" value="Search"/>													
NO	Time	DropEvents	Octets	Pkts	BroadcastPkts	MulticastPkts	CRCAlignErrors	UndersizePkts	OversizePkts	Fragments	Jabbers	Collisions	Utilization
1	2000-4-26 16:43:22	0	0	0	0	0	0	0	0	0	0	0	0%
<input type="button" value="Back"/> <input type="button" value="Refresh"/>													

2. Fields of RMON history sampling information

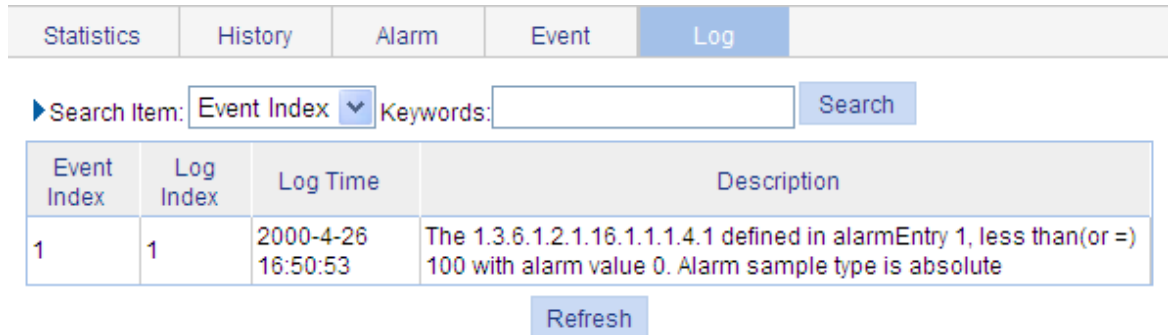
Item	Description
NO	Number of the entry in the system buffer Statistics are numbered chronologically when they are saved to the system buffer.
Time	Time at which the information is saved
DropEvents	Dropped packets during the sampling period, corresponding to the MIB node etherHistoryDropEvents.
Octets	Number of octets received during the sampling period, corresponding to the MIB node etherHistoryOctets.
Pkts	Number of packets received during the sampling period, corresponding to the MIB node etherHistoryPkts.
BroadcastPkts	Number of broadcasts received during the sampling period, corresponding to the MIB node etherHistoryBroadcastPkts.
MulticastPkts	Number of multicasts received during the sampling period, corresponding to the MIB node etherHistoryMulticastPkts.
CRCAlignErrors	Number of packets received with CRC alignment errors during the sampling period, corresponding to the MIB node etherHistoryCRCAlignErrors.
UndersizePkts	Number of undersize packets received during the sampling period, corresponding to the MIB node etherHistoryUndersizePkts.
OversizePkts	Number of oversize packets received during the sampling period, corresponding to the MIB node etherHistoryOversizePkts.
Fragments	Number of fragments received during the sampling period, corresponding to the MIB node etherHistoryFragments.
Jabbers	Number of jabbers received during the sampling period (Support for the field depends on the device model.), corresponding to the MIB node etherHistoryJabbers.
Collisions	Number of collision packets received during the sampling period, corresponding to the MIB node etherHistoryCollisions.
Utilization	Bandwidth utilization during the sampling period, corresponding to the MIB node etherHistoryUtilization.

Return to [Display RMON running status.](#)

Displaying RMON event logs

Select **Device** → **RMON** from the navigation tree and click the **Log** tab to enter the page, as shown in [a](#), which displays log information for all event entries.

a. Log



The screenshot shows the RMON Log page with a navigation bar containing tabs for Statistics, History, Alarm, Event, and Log. Below the tabs is a search section with a dropdown menu set to 'Event Index', a text input for 'Keywords', and a 'Search' button. A table displays the log entries with columns for Event Index, Log Index, Log Time, and Description. Below the table is a 'Refresh' button.

Event Index	Log Index	Log Time	Description
1	1	2000-4-26 16:50:53	The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarmEntry 1, less than(or =) 100 with alarm value 0. Alarm sample type is absolute

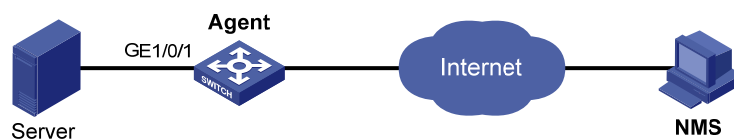
Return to [Display RMON running status](#).

RMON configuration example

Network requirements

As shown in [a](#), Agent is connected to a remote NMS across the Internet. Create an entry in the RMON Ethernet statistics table to gather statistics on Ethernet 1/0/1, and perform corresponding configurations so that the system will log the event when the number of bytes received on the interface exceed the specified threshold.

a. Network diagram for RMON



Configuration procedure

Configure RMON to gather statistics for interface Ethernet 1/0/1.

- Select **Device** → **RMON** from the navigation tree to enter the page of the **Statistics** tab. Click **Add**.

a. Add a statistics entry



Add a Statistic Group

Interface Name:	GigabitEthernet1/0/1	▼
Owner:	user1-rmon	Chars.(1-127)


- Only one statistics group can be created on one interface.

Items marked with an asterisk(*) are required



- Select **GigabitEthernet1/0/1** from the **Interface Name** drop-down box.
- Type **user1-rmon** in the text box of **Owner**.
- Click **Apply**.

Display RMON statistics for interface Ethernet 1/0/1.

- Click the icon  corresponding to GigabitEthernet 1/0/1.
- You can view the information as shown in [b](#).

b. Display RMON statistics

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

Statistic Group Detail

Current Interface: GigabitEthernet1/0/1

Statistic Item	Statistic Value
Number of Received Bytes	21657
Number of Received Packets	307
Number of Received Broadcasting Packets	56
Number of Received Multicast Packets	34
Number of Received Packets With CRC Check Failed	0
Number of Received Packets Smaller Than 64 Bytes	0
Number of Received Packets Larger Than 1518 Bytes	0
Number of Received Packets Smaller Than 64 Bytes And FCS Check Failed	0
Number of Received Packets Larger Than 1518 Bytes And FCS Check Failed	0
Number of Network Conflicts	0
Number of Packet Discarding Events	0
Number of Received 64 Bytes Packets	235
Number of Received 65 to 127 Bytes Packets	67
Number of Received 128 to 255 Bytes Packets	4
Number of Received 256 to 511 Bytes Packets	1
Number of Received 512 to 1023 Bytes Packets	0
Number of Received 1024 to 1518 Bytes Packets	0

[Back](#) [Refresh](#)

Create an event to start logging after the event is triggered.

- Click the **Event** tab, click **Add**.

c. Configure an event group

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

Add an Event Group

Description: Chars.(1-127)

Owner: Chars.(1-127)

Event Type: Log Trap

Items marked with an asterisk(*) are required

- Type **1-rmon** in the text box of **Owner**.
- Select the check box before **Log**.
- Click **Apply**.
- The page goes to the page displaying the event entry, and you can see that the entry index of the new event is **1**, as shown in **d**.

d. Display the index of a event entry

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

► Search Item: Keywords:

<input type="checkbox"/>	Index	Description	Event Type	Event Last Trigger Time	Owner	Status
<input type="checkbox"/>	1	null	Log	-	1-rmon	Active

Configure an alarm group to sample received bytes on Ethernet 1/0/1. When the received bytes exceed the rising or falling threshold, logging is enabled.

- Click the **Alarm** tab, click **Add**.

e. **Configure an alarm group**

Statistics	History	Alarm	Event	Log	
------------	---------	-------	-------	-----	--

Add an Alarm Group

Alarm Variable

Statics Item:

Interface Name:

Sample Item

Interval: *Seconds(5-65535)

Sample Type:

Owner: Chars.(1-127)

Alarm

Create Default Event

Rising Threshold: *(0-2147483647) Rising Event:

Falling Threshold: *(0-2147483647) Falling Event:

- Before creating Alarm, please create Statistic and Event at first.

Items marked with an asterisk(*) are required

- Select **Number of Received Bytes** from the **Statics Item** drop-down box.
- Select **GigabitEthernet1/0/1** from the **Interface Name** drop-down box.
- Type **10** in the text box of **Interval**.
- Select **Delta** from the **Simple Type** drop-down box.
- Type **1-rmon** in the text box of **Owner**.
- Type **1000** in the text box of **Rising Threshold**.
- Select **1** from the **Rising Event** drop-down box.
- Type **100** in the text box of **Falling Threshold**.
- Select **1** from the **Falling Event** drop-down box.
- Click **Apply**.

Energy saving configuration

Overview

Energy saving allows you to configure a port to work at the lowest transmission speed, disable PoE, or go down during a specified time range on certain days of a week. The port resumes working normally when the effective time period ends.

Configuring energy saving on a port

Select **Device** → **Energy Saving** from the navigation tree to enter the energy saving configuration page, as shown in a. You can select a port and configure an energy saving policy for the port.

a. Energy saving configuration page

Index	Time Range	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Lowest Speed	Shutdown
1	20:00-24:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	00:00-00:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	00:00-00:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Configuration items for configuring energy saving on a port

Item	Description
Time Range	Set the time period when the port is in the state of energy saving. ! IMPORTANT: <ul style="list-style-type: none">Up to five energy saving policies with different time ranges can be configured on a port.Specify the start time and end time in units of 5 minutes, such as 08:05 to 10:15. Otherwise, the start time will be postponed and the end time will be brought forward so that they meet the requirements. For example, if you set the time range to 08:08 to 10:12, however, the effective time range is actually 08:10 to 10:10.
Sun through Sat	
PoE Disabled	Disable PoE on the port.

Item	Description
Lowest Speed	<p>Set the port to transmit data at the lowest speed.</p> <p>ⓘ IMPORTANT:</p> <p>If you configure the lowest speed limit on a port that does not support 10 Mbps, the configuration cannot take effect.</p>
Shutdown	<p>Shut down the port.</p> <p>ⓘ IMPORTANT:</p> <p>An energy saving policy can have all the three energy saving schemes configured, of which the shutdown scheme takes the highest priority.</p>

SNMP configuration

The Simple Network Management Protocol (SNMP) is an Internet standard protocol widely used for a management station to access and operate the devices on a network, regardless of their vendors, physical characteristics and interconnect technologies.

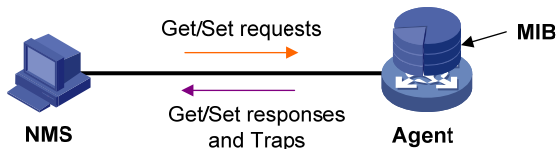
SNMP enables network administrators to read and set the variables on managed devices to monitor their operating and health state, diagnose network problems, and collect statistics for management purposes.

SNMP mechanism

The SNMP framework comprises the following elements:

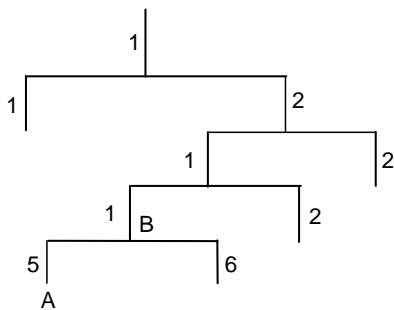
- SNMP manager—works on a network management workstation (NMS) to monitor and manage the SNMP-capable devices in the network.
- SNMP agent—works on a managed device to receive and handle requests from the NMS, and send traps to the NMS when some events, such as interface state change, occur.
- Management Information Base (MIB)—Specifies the variables (such as interface status and CPU usage) maintained by the SNMP agent for the SNMP manager to read and set.

a. Relationship between an NMS, agent and MIB



A MIB stores variables called “nodes” or “objects” in a tree hierarchy and identifies each node with a unique OID. An OID is a string of numbers that describes the path from the root node to a leaf node. For example, the object B in **b** is uniquely identified by the OID {1.2.1.1}.

b. MIB tree



SNMP provides the following four basic operations:

- Get—The NMS retrieves SNMP object nodes in an agent MIB.
- Set—The NMS modifies the value of an object node in the agent MIB.
- Trap—The SNMP agent sends traps to report events to the NMS.
- Inform—The NMS sends alarms to other NMSs.

SNMP protocol version

SNMP agents support three SNMP protocol versions: SNMPv1, SNMPv2c, and SNMPv3.

- SNMPv1 uses community names for authentication. A community name performs a similar role as a password to regulate access from the NMS to the agent. If the community name provided by the NMS is different from the community name set on the agent, the SNMP connection cannot be established and the NMS fails to access the agent.
- SNMPv2c uses community names for authentication. SNMPv2c is compatible with SNMPv1, but it provides more operation modes, supports more data types, and provides various error codes for troubleshooting.
- SNMPv3 offers authentication based on the User-based Security Model (USM), which allows network administrators to set authentication and privacy functions. The authentication function is used to authenticate the validity of the sending end of the authentication packets, preventing access of unauthorized users. The privacy function is used to encrypt packets between the NMS and agents, preventing the packets from being intercepted. USM ensures more secure communication between NMSs and agents by providing authentication and privacy functions.

Successful interaction between an NMS and the agents requires consistency of SNMP versions configured on them.

SNMP configuration

Configuration task list

As configurations for SNMPv3 differ substantially from those for SNMPv1 and SNMPv2c, their configuration tasks are introduced separately as follows.

Configuring SNMPv1 or SNMPv2c

Perform the tasks in 1 to configure SNMPv1 or SNMPv2c:

1. SNMPv1 or SNMPv2c configuration task list

Task	Remarks
Enabling SNMP	Required The SNMP agent function is disabled by default. ⚠ IMPORTANT: If SNMP is disabled, all SNMP-related configurations are removed.
Configuring an SNMP	Optional After creating SNMP views, you can specify an SNMP view for an SNMP community to limit the MIB objects that can be accessed by the SNMP community.
Configuring an SNMP	Required

Task	Remarks
Configuring SNMP trap	Optional Allows you to configure that the agent can send SNMP traps to the NMS, and configure information about the target host of the SNMP traps. By default, an agent is allowed to send SNMP traps to the NMS.

Configuring SNMPv3

Perform the tasks in 1 to configure SNMPv3:

1. SNMPv3 configuration task list

Task	Remarks
Enabling SNMP	Required The SNMP agent function is disabled by default.
Configuring an SNMP	Optional After creating SNMP views, you can specify an SNMP view for an SNMP group to limit the MIB objects that can be accessed by the SNMP group.
Configuring an SNMP	Required After creating an SNMP group, you can add SNMP users to the group when creating the users. Therefore, you can realize centralized management of users in the group through the management of the group.
Configuring an SNMP	Required Before creating an SNMP user, you need to create the SNMP group to which the user belongs.
Configuring SNMP trap	Optional Allows you to configure that the agent can send SNMP traps to the NMS, and configure information about the target host of the SNMP traps By default, an agent is allowed to send SNMP traps to the NMS.

Enabling SNMP

Select **Device** → **SNMP** from the navigation tree to enter the SNMP configuration page, as shown in a. On the upper part of the page, you can select to enable or disable SNMP and configure parameters such as SNMP version; on the lower part of the page, you can view the SNMP statistics, which helps you understand the running status of the SNMP after your configuration.

a. Set up

Setup	Community	Group	User	Trap	View
SNMP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable				
Local Engine ID	<input type="text" value="8000002B03000FE2012970"/> *(10-64 Hex Chars.)				
Maximum Packet Size	<input type="text" value="1500"/> *Bytes(484-17940, Default = 1500)				
Contact	<input type="text" value="3Com Corporation."/> *(1-200 Chars.)				
Location	<input type="text" value="Marlborough, MA 01752 USA"/> *(1-200 Chars.)				
SNMP Version	<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input checked="" type="checkbox"/> v3				

Items marked with an asterisk(*) are required

Apply Cancel

SNMP Statistics	Count
Messages delivered to the SNMP entity	0
Messages which were for an unsupported version	0
Messages which used a SNMP community name not known	0
Messages which represented an illegal operation for the community supplied	0
ASN.1 or BER errors in the process of decoding	0
MIB objects retrieved successfully	0
MIB objects altered successfully	0
GetRequest-PDU accepted and processed	0
GetNextRequest-PDU accepted and processed	0
SetRequest-PDU accepted and processed	0
Messages passed from the SNMP entity	0
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	0
SNMP PDUs which had noSuchName error-status	0
SNMP PDUs which had badValue error-status	0
SNMP PDUs which had genErr error-status	0
GetResponse-PDU accepted and processed	0
Trap PDUs accepted and processed	0

Refresh

2. Configuration items for enabling SNMP

Item	Description
SNMP	Specify to enable or disable SNMP.
Local Engine ID	Configure the local engine ID. The validity of a user after it is created depends on the engine ID of the SNMP agent. If the engine ID when the user is created is not identical to the current engine ID, the user is invalid.
Maximum Packet Size	Configure the maximum size of an SNMP packet that the agent can receive/send.

Item	Description
Contact	Set a character string to describe the contact information for system maintenance. If the device is faulty, the maintainer can contact the manufacture factory according to the contact information of the device.
Location	Set a character string to describe the physical location of the device.
SNMP Version	Set the SNMP version run by the system

Return to [SNMPv1 or SNMPv2c configuration task list](#) or [SNMPv3 configuration task list](#).

Configuring an SNMP view

Select **Device** → **SNMP** from the navigation tree, and then click the **View** tab to enter the page as shown in a.

a. View page

View Name	Rule	MIB Subtree OID	Subtree Mask	Operation
ViewDefault				
	Included	1		
	Excluded	1.3.6.1.6.3.15		
	Excluded	1.3.6.1.6.3.16		
	Excluded	1.3.6.1.6.3.18		

Add

Creating an SNMP view

Table 23 Click **Add**, the **Add View** window appears as shown in b.

Table 24 Type the view name and click **Apply**, and then you enter the page as shown in c.

b. Create an SNMP view (1)

Please input the name of the view you want to create.

View Name (1-32 Chars.)

c. Create an SNMP view (2)

Add View

View Name

Rule Included Excluded

MIB Subtree OID *(1-255 Chars.)

Subtree Mask (2-32Hex Chars.)

Items marked with an asterisk(*) are required

Rule	MIB Subtree OID	Subtree Mask	Operation

Table 25 Configure the parameters of a rule and click **Add** to add the rule into the list box at the lower part of the page.

Table 26 Configure all rules and click **Apply** to create an SNMP view. Note that the view will not be created if you click **Cancel**.

2. Configuration items for creating an SNMP view

Item	Description
View Name	Set the SNMP view name.
Rule	Select to exclude or include the objects in the view range determined by the MIB subtree OID and subtree mask.
MIB Subtree OID	Set the MIB subtree OID (such as 1.4.5.3.1) or name (such as system). MIB subtree OID identifies the position of a node in the MIB tree, and it can uniquely identify a MIB subtree.
Subtree Mask	Set the subtree mask. If no subtree mask is specified, the default subtree mask (all Fs) will be used for mask-OID matching.

Adding rules to an SNMP view


Table 27 Click the  icon corresponding to the specified view on the page as shown in a, the **Add rule for the view ViewDefault** window appears as shown in b.

Table 28 Configure the parameters, and click **Apply** to add the rule for the view. 2 describes the configuration items for creating an SNMP view.

b. Add rules to an SNMP view

Add rule for the view ViewDefault


Rule Included Excluded

MIB Subtree OID *(1-255 Chars.)

Subtree Mask (2-32Hex Chars.)

Items marked with an asterisk(*) are required

NOTE:

You can also click the  icon corresponding to the specified view on the page as shown in [a](#), and then you can enter the page to modify the view.

Return to [SNMPv1](#) or [SNMPv2c](#) configuration task list or [SNMPv3](#) configuration task list.

Configuring an SNMP community

Table 29 Select **Device** → **SNMP** from the navigation tree.



Table 30 Click the **Community** tab to enter the page as shown in [b](#).

Table 31 Click **Add** to enter the **Add SNMP Community** page as shown in [c](#).

b. Configure an SNMP community

Setup	Community	Group	User	Trap	View	
-------	------------------	-------	------	------	------	--

▶ Search Item: Keywords:

<input type="checkbox"/>	Community Name	Access Right	MIB View	ACL	Operation
<input type="checkbox"/>	community1	Read only	ViewDefault		 

c. Create an SNMP Community

Add SNMP Community

Community Name *(1-32 Chars.)

Access Right

View

ACL (2000-2999)

Items marked with an asterisk(*) are required

2. Configuration items for configuring an SNMP community

Item	Description
Community Name	Set the SNMP community name.
Access Right	Configure SNMP NMS access right <ul style="list-style-type: none"> • Read only—The NMS can perform read-only operations to the MIB objects when it uses this community name to access the agent, • Read and write—The NMS can perform both read and write operations to the MIB objects when it uses this community name to access the agent.
View	Specify the view associated with the community to limit the MIB objects that can be accessed by the NMS.
ACL	Associate the community with a basic ACL to allow or prohibit the access to the agent from the NMS with the specified source IP address.

Return to [SNMPv1](#) or [SNMPv2c](#) configuration task list.



Configuring an SNMP group

Table 32 Select **Device** → **SNMP** from the navigation tree.

Table 33 Click the **Group** tab to enter the page as shown in **b**.

Table 34 Click **Add** to enter the **Add SNMP Group** page as shown in **c**.

b. SNMP group

Setup	Community	Group	User	Trap	View		
▶ Search Item: <input type="text" value="Group Name"/> Keywords: <input type="text"/>				<input type="button" value="Search"/>			
<input type="checkbox"/>	Group Name	Security Level	Read View	Write View	Notify View	ACL	Operation
<input type="checkbox"/>	group1	NoAuth/NoPriv	ViewDefault	ViewDefault	ViewDefault		 
		<input type="button" value="Add"/>		<input type="button" value="Delete Selected"/>			

c. Create an SNMP group

Add SNMP Group

Group Name	<input type="text"/>	*(1-32 Chars.)
Security Level	<input type="text" value="NoAuth/NoPriv"/>	▼
Read View	<input type="text" value="ViewDefault"/>	▼
Write View	<input type="text"/>	▼
Notify View	<input type="text"/>	▼
ACL	<input type="text"/>	(2000-2999)

Items marked with an asterisk(*) are required

Apply

Cancel

2. Configuration items for creating an SNMP group

Item	Description
Group Name	Set the SNMP group name.
Security Level	Select the security level for the SNMP group. The available security levels are: <ul style="list-style-type: none">• NoAuth/NoPriv—No authentication no privacy.• Auth/NoPriv—Authentication without privacy.• Auth/Priv—Authentication and privacy. <p>! IMPORTANT: For an existing SNMP group, its security level cannot be modified.</p>
Read View	Select the read view of the SNMP group.
Write View	Select the write view of the SNMP group. If no write view is configured, the NMS cannot perform the write operations to all MIB objects on the device.
Notify View	Select the notify view of the SNMP group, that is, the view that can send trap messages. If no notify view is configured, the agent does not send traps to the NMS.
ACL	Associate a basic ACL with the group to restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to restrict the intercommunication between the NMS and the agent.

Return to [SNMPv3 configuration task list](#).

Configuring an SNMP user

Table 35 Select **Device** → **SNMP** from the navigation tree.

Table 36 Click the **User** tab to enter the page as shown in [b](#).

Table 37 Click **Add** to enter the **Add SNMP User** page, as shown in [c](#).

b. SNMP user

Setup	Community	Group	User	Trap	View	
▶ Search Item: <input type="text" value="User Name"/> Keywords: <input type="text"/> <input type="button" value="Search"/>						
<input type="checkbox"/>	User Name	Group Name	Authentication Mode	Privacy Mode	ACL	Operation
<input type="checkbox"/>	user1	group1 (NoAuth/NoPriv)	MD5	DES56		
			<input type="button" value="Add"/>	<input type="button" value="Delete Selected"/>		

c. Create an SNMP user

Add SNMP User

User Name	<input type="text"/>	*(1-32 Chars.)
Security Level	<input type="text" value="NoAuth/NoPriv"/>	
Group Name	<input type="text" value="group1 (NoAuth/NoPriv)"/>	
Authentication Mode	<input type="text" value="MD5"/>	
Authentication Password	<input type="text"/>	(1-64 Chars.)
Confirm Authentication Password	<input type="text"/>	(1-64 Chars.)
Privacy Mode	<input type="text" value="DES56"/>	
Privacy Password	<input type="text"/>	(1-64 Chars.)
Confirm Privacy Password	<input type="text"/>	(1-64 Chars.)
ACL	<input type="text"/>	(2000-2999)

Items marked with an asterisk(*) are required

2. Configuration items for creating an SNMP user

Item	Description
User Name	Set the SNMP user name.
Security Level	Select the security level for the SNMP group. The following are the available security levels: <ul style="list-style-type: none"> NoAuth/NoPriv—No authentication no privacy. Auth/NoPriv—Authentication without privacy. Auth/Priv—Authentication and privacy.

Item	Description
Group Name	<p>Select an SNMP group to which the user belongs.</p> <ul style="list-style-type: none"> • When the security level is NoAuth/NoPriv, you can select an SNMP group with no authentication no privacy. • When the security level is Auth/NoPriv, you can select an SNMP group with no authentication no privacy or authentication without privacy. • When the security level is Auth/Priv, you can select an SNMP group of any security level.
Authentication Mode	Select an authentication mode (including MD5 and SHA) when the security level is Auth/NoPriv or Auth/Priv.
Authentication Password	Set the authentication password when the security level is Auth/NoPriv or Auth/Priv.
Confirm Authentication Password	The confirm authentication password must be the same with the authentication password.
Privacy Mode	Select a privacy mode (including DES56, AES128, and 3DES) when the security level is Auth/Priv.
Privacy Password	Set the privacy password when the security level is Auth/Priv.
Confirm Privacy Password	The confirm privacy password must be the same with the privacy password.
ACL	Associate a basic ACL with the user to restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to allow or prohibit the specified NMS to access the agent by using this user name.

Return to [SNMPv3 configuration task list](#).

Configuring SNMP trap function

Table 38 Select **Device** → **SNMP** from the navigation tree.

Table 39 Click the **Trap** tab to enter the page as shown in [b](#).

Table 40 On the upper part of the page, you can select to enable the SNMP trap function; on the lower part of the page, you can configure target hosts of the SNMP traps.

Table 41 Click **Add** to enter the **Add Trap Target Host** page, as shown in [c](#).

b. Traps configuration

Setup	Community	Group	User	Trap	View
-------	-----------	-------	------	------	------

Enable SNMP Trap Apply

Trap Target Host

▶ Search Item: Destination IP Address ▼ Keywords: Search

<input type="checkbox"/>	Destination IP Address	IPv4/IPv6	Security Name	UDP Port	Security Model	Security Level	Operation
<input type="checkbox"/>	10.1.1.2	IPv4	abc	162	v3	Auth/NoPriv	

Add Delete Selected

c. Add a target host of SNMP traps

Setup	Community	Group	User	Trap	View
-------	-----------	-------	------	------	------

Add Trap Target Host

Destination IP Address IPv4 IPv6

*

Security Name *(1-32 Chars.)

UDP Port *(0-65535, Default = 162)

Security Model ▼

Security Level ▼

Items marked with an asterisk(*) are required

Apply Cancel

2. Configuration items for adding a target host

Item	Description
Destination IP Address	Set the destination IP address. Select the IP address type: IPv4 or IPv6, and then type the corresponding IP address in the text box according to the IP address type.
Security Name	Set the security name, which can be an SNMPv1 community name, an SNMPv2c community name, or an SNMPv3 user name.

Item	Description
UDP Port	<p>Set UDP port number.</p> <p>! IMPORTANT:</p> <p>The default port number is 162, which is the SNMP-specified port used for receiving traps on the NMS. Generally (such as using iMC or MIB Browser as the NMS), you can use the default port number. To change this parameter to another value, you need to make sure that the configuration is the same with that on the NMS.</p>
Security Model	<p>Select the security model, that is, the SNMP version. Ensure that the SNMP version is the same with that on the NMS; otherwise, the NMS cannot receive any trap.</p>
Security Level	<p>Set the authentication and privacy mode for SNMP traps when the security model is selected as v3. The available security levels are: no authentication no privacy, authentication but no privacy, and authentication and privacy.</p> <p>When the security model is selected as v1 or v2c, the security level is no authentication no privacy, and cannot be modified.</p>

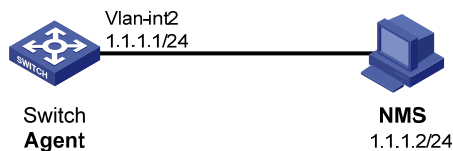
Return to [SNMPv1 or SNMPv2c configuration task list](#) or [SNMPv3 configuration task list](#).

SNMP configuration example

Network requirements

- As shown in [a](#), the NMS connects to the agent, Switch, through an Ethernet.
- The IP address of the NMS is 1.1.1.2/24.
- The IP address of the VLAN interface on Switch is 1.1.1.1/24.
- The NMS monitors the agent using SNMPv3. The agent reports errors or faults to the NMS.

a. Network diagram for SNMP configuration



Configuration procedure

Table 42 Configure Agent

Configuration IP addresses for the interfaces. (Procedure omitted)

Enable SNMP.

- Select **Device** → **SNMP** from the navigation tree to enter the **Setup** page.

b. Enable SNMP

Setup	Community	Group	User	Trap	View
SNMP <input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Local Engine ID	800063A2033CE5A61238DD		*(10-64 Hex Chars.)		
Maximum Packet Size	1500		*Bytes(484-17940, Default = 1500)		
Contact	HP		*(1-200 Chars.)		
Location	HP		*(1-200 Chars.)		
SNMP Version	<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input checked="" type="checkbox"/> v3				
Items marked with an asterisk(*) are required					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					
SNMP Statistics					Count
Messages delivered to the SNMP entity					0
Messages which were for an unsupported version					0
Messages which used a SNMP community name not known					0

- Select the **Enable** radio box.
- Select the **v3** radio box.
- Click **Apply**.

Configure an SNMP view.

- Click the **View** tab and then click **Add** to enter the page as shown in c.

c. Create an SNMP view (1)

Please input the name of the view you want to create.

View Name (1-32 Chars.)



- Type **view1** in the text box.
- Click **Apply** to enter the SNMP rule configuration page, as shown in d.

d. Create an SNMP view (2)

Add View

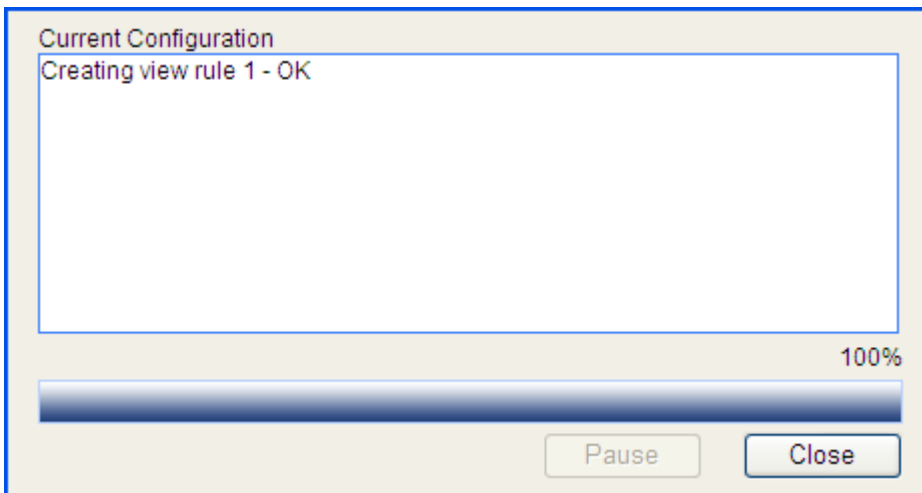
View Name	view1
Rule	<input checked="" type="radio"/> Included <input type="radio"/> Excluded
MIB Subtree OID	interfaces <small>*(1-255 Chars.)</small>
Subtree Mask	<input type="text"/> <small>(2-32Hex Chars.)</small>

Items marked with an asterisk(*) are required

Rule	MIB Subtree OID	Subtree Mask	Operation
Included	interfaces		 

- Select the **Included** radio box.
- Type the MIB subtree OID **interfaces**.
- Click **Add**.
- Click **Apply**. A configuration progress dialog box appears, as shown in e.

e. Configuration progress dialog box



Current Configuration
Creating view rule 1 - OK

100%

- After the configuration process is complete, click **Close**.
- # Configure an SNMP group.
- Click the **Group** tab and then click **Add** to enter the page as shown in f.

f. **Create an SNMP group**

Add SNMP Group

Group Name	<input type="text" value="group1"/> *(1-32 Chars.)
Security Level	NoAuth/NoPriv ▼
Read View	view1 ▼
Write View	view1 ▼
Notify View	▼
ACL	<input type="text"/> (2000-2999)

Items marked with an asterisk(*) are required

- Type **group1** in the text box of **Group Name**.
- Select **view1** from the **Read View** drop-down box.
- Select **view1** from the **Write View** drop-down box.
- Click **Apply**.

Configure an SNMP user

- Click the **User** tab and then click **Add** to enter the page as shown in g.

g. **Create an SNMP user**

Add SNMP User

User Name	<input type="text" value="user1"/> *(1-32 Chars.)
Security Level	NoAuth/NoPriv ▼
Group Name	group1 (NoAuth/NoPriv) ▼
Authentication Mode	MD5 ▼
Authentication Password	<input type="text"/> (1-64 Chars.)
Confirm Authentication Password	<input type="text"/> (1-64 Chars.)
Privacy Mode	DES56 ▼
Privacy Password	<input type="text"/> (1-64 Chars.)
Confirm Privacy Password	<input type="text"/> (1-64 Chars.)
ACL	<input type="text"/> (2000-2999)

Items marked with an asterisk(*) are required

- Type **user1** in the text box of **User Name**.
- Select **group1** from the **Group Name** drop-down box.

- Click **Apply**.
- # Enable the agent to send SNMP traps.
- Click the **Trap** tab and enter the page as shown in [h](#).

h. Enable the agent to send SNMP traps

Setup	Community	Group	User	Trap	View	
-------	-----------	-------	------	------	------	--

Enable SNMP Trap

Trap Target Host

▶ Search Item: Destination IP Address Keywords:

<input type="checkbox"/>	Destination IP Address	IPv4/IPv6	Security Name	UDP Port	Security Model	Security Level	Operation

- Select the **Enable SNMP Trap** check-box.
- Click **Apply**.
- # Add the target hosts of SNMP traps.
- Click **Add** to enter the page as shown in [i](#).

i. Add target hosts of SNMP traps

Add Trap Target Host

Destination IP Address IPv4 IPv6

*

Security Name *(1-32 Chars.)

UDP Port *(0-65535, Default = 162)

Security Model ▼

Security Level ▼

Items marked with an asterisk(*) are required

- Select the destination IP address type as **IPv4**.
- Type the destination address **1.1.1.2**.
- Type the user name **user1**.
- Select **v3** from the **Security Model** drop-down box.
- Click **Apply**.

Table 43 Configure NMS.

△ CAUTION:

The configuration on NMS must be consistent with that on the agent. Otherwise, you cannot perform corresponding operations.

SNMPv3 adopts a security mechanism of authentication and privacy. You must configure the username and security level. According to the configured security level, you must also configure the related authentication mode, authentication password, privacy mode, privacy password, and so on.

You must also configure the aging time and retry times. After these configurations, you can configure the device as needed through the NMS. For more information about NMS configuration, see the manual provided for NMS.

Configuration verification

- After the above configuration, the NMS can establish an SNMP connection with the agent and query and reconfigure values of objects in the agent MIB.
- If an idle interface on the agent is shut down or brought up, the NMS receives trap information sent by the agent.

Interface statistics

Overview

The interface statistics module displays statistics information about the packets received and sent through interfaces.

Displaying interface statistics

Select **Device** → **Interface Statistics** from the navigation tree to enter the interface statistics display page, as shown in a.

a. Interface statistics display page

Interface Statistics

Search Item: Keywords:

<input type="checkbox"/>	Interface Name	InOctets	InUcastPkts	InNUcastPkts	InDiscards	InErrors	InUnknownProtos	OutOctets	OutUcastPkts	OutNUcastPkts	OutDiscards	OutErrors	Last statistics clearing time
<input type="checkbox"/>	GigabitEthernet1/0/1	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/2	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/3	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/4	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/5	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/6	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/7	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/8	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/9	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/10	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/11	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/12	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/13	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/14	0	0	0	0	0	0	0	0	0	0	0	-
<input type="checkbox"/>	GigabitEthernet1/0/15	8167	30	18	0	0	0	34632	37	0	0	0	2000-4-26 19:06:41

22 records, 15 per page | page 1/2, record 1-15 | [First](#) [Prev](#) [Next](#) [Last](#) 1

2. Details about the interface statistics

Field	Description
InOctets	Total octets of all packets received on the interface.
InUcastPkts	Number of received unicast packets.
InNUcastPkts	Number of received non-unicast packets.
InDiscards	Number of valid packets discarded in the inbound direction.
InErrors	Number of received invalid packets.
InUnknownProtos	Number of received unknown protocol packets.
OutOctets	Total octets of all packets sent through the interface.

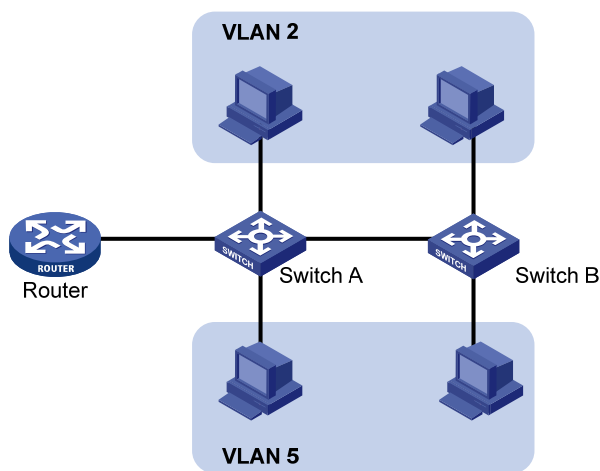
Field	Description
OutUcastPkts	Number of unicast packets sent through the interface.
OutNUcastPkts	Number of non-unicast packets sent through the interface.
OutDiscards	Number of valid packets discarded in the outbound direction.
OutErrors	Number of invalid packets sent through the interface.

VLAN configuration

Introduction to VLAN

Ethernet is a network technology based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) mechanism. As the medium is shared, collisions and excessive broadcasts are common on Ethernet networks. To address the issue, virtual LAN (VLAN) was introduced to break a LAN down into separate VLANs. VLANs are isolated from each other at Layer 2. A VLAN is a bridging domain, and all broadcast traffic is contained within it, as shown in a.

a. A VLAN diagram



A VLAN is logically divided on an organizational basis rather than on a physical basis. For example, all workstations and servers used by a particular workgroup can be connected to the same LAN, regardless of their physical locations.

VLAN technology delivers the following benefits:

- Confining broadcast traffic within individual VLANs. This reduces bandwidth waste and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. To enable communication between VLANs, routers or Layer 3 switches are required.
- Flexible virtual workgroup creation. As users from the same workgroup can be assigned to the same VLAN regardless of their physical locations, network construction and maintenance is much easier and more flexible.

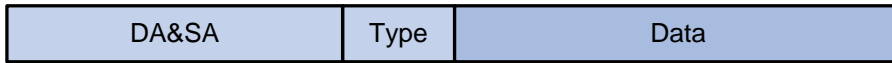
VLAN fundamentals

To enable a network device to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation.

The format of VLAN-tagged frames is defined in IEEE 802.1Q issued by the Institute of Electrical and Electronics Engineers (IEEE) in 1999.

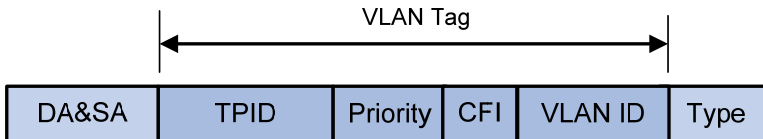
In the header of a traditional Ethernet data frame, the field after the destination MAC address and the source MAC address is the Type field indicating the upper layer protocol type, as shown in [a](#).

a. Traditional Ethernet frame format



IEEE 802.1Q inserts a four-byte VLAN tag after the DA&SA field, as shown in [b](#).

b. Position and format of VLAN tag



A VLAN tag comprises the following fields: tag protocol identifier (TPID), priority, canonical format indicator (CFI), and VLAN ID.

- The 16-bit TPID field with a value of 0x8100 indicates that the frame is VLAN tagged.
- The 3-bit priority field indicates the 802.1p priority of the frame.
- The 1-bit CFI field specifies whether the MAC addresses are encapsulated in the standard format when packets are transmitted across different media. A value of 0 indicates that the MAC addresses are encapsulated in canonical format. A value of 1 indicates that the MAC addresses are encapsulated in a non-standard format. The value of the field is 0 by default.
- The 12-bit VLAN ID field identifies the VLAN the frame belongs to. The VLAN ID range is 0 to 4095. As 0 and 4095 are reserved, a VLAN ID actually ranges from 1 to 4094.

A network device handles an incoming frame depending on whether the frame is VLAN tagged and the value of the VLAN tag, if any. For more information, see [“Introduction to port-based VLAN”](#).

NOTE:

The Ethernet II encapsulation format is used here. Besides the Ethernet II encapsulation format, Ethernet also supports other encapsulation formats, including 802.2 LLC, 802.2 SNAP, and 802.3 raw. The VLAN tag fields are added to frames encapsulated in these formats for VLAN identification.

VLAN types

You can implement VLANs based on the following criteria:

- Port
- MAC address
- Protocol
- IP subnet
- Policy
- Other criteria

The web interface is available only for port-based VLANs, and this chapter introduces only port-based VLANs.

Introduction to port-based VLAN

Port-based VLANs group VLAN members by port. A port forwards traffic for a VLAN only after it is assigned to the VLAN.

Port link type

You can configure the link type of a port as access, trunk, or hybrid. The link types use the following VLAN tag handling methods:

- An access port belongs to only one VLAN and sends traffic untagged. It is usually connects to a user device unable to recognize VLAN tagged-packets or when there is no need to separate different VLAN members.
- A trunk port can carry multiple VLANs to receive and send traffic for them. Except traffic from the port VLAN ID (PVID), traffic sent through a trunk port will be VLAN tagged. Usually, ports connecting network devices are configured as trunk ports.
- Like a trunk port, a hybrid port can carry multiple VLANs to receive and send traffic for them. Unlike a trunk port, a hybrid port allows traffic of all VLANs to pass through VLAN untagged. Usually, hybrid ports are configured to connect devices whose support for VLAN tagged-packets you are uncertain about.

PVID

By default, VLAN 1 is the PVID for all ports. You can change the PVID for a port as required.

Use the following guidelines when configuring the PVID on a port:

- An access port can join only one VLAN. The VLAN to which the access port belongs is the PVID of the port. The PVID of the access port changes along with the VLAN to which the port belongs.
- A trunk or hybrid port can join multiple VLANs, and you can configure a PVID for the port.

The following table shows how ports of different link types handle frames:

Port type	Actions (in the inbound direction)		Actions (in the outbound direction)
	Untagged frame	Tagged frame	
Access	Tags the frame with the PVID tag.	<ul style="list-style-type: none">• Receives the frame if its VLAN ID is the same as the PVID.• Drops the frame if its VLAN ID is different from the PVID.	Removes the VLAN tag and sends the frame.
Trunk	Checks whether the PVID is carried on the port: <ul style="list-style-type: none">• If yes, tags the frame with the PVID tag.	<ul style="list-style-type: none">• Receives the frame if its VLAN is carried on the port.• Drops the frame if its VLAN is not carried on the port.	<ul style="list-style-type: none">• Removes the tag and sends the frame if the frame carries the PVID tag and the port belongs to the PVID.• Sends the frame without removing the tag if its VLAN is carried on the port but is different from the PVID.
Hybrid	<ul style="list-style-type: none">• If not, drops the frame.		Sends the frame if its VLAN is carried on the port. The frame is sent with the VLAN tag removed or intact depending on your configuration.

Configuring a VLAN

Configuration task list

Use either of the following approaches or the combination of them to configure a VLAN, as shown in 1 and 2:

1. VLAN configuration task list (approach I)

Task	Remarks
Creating VLANs	Required Create one or multiple VLANs.
Selecting VLANs	Required Configure a subset of all existing VLANs. This step is required before displaying, modifying, or removing a VLAN.
Modifying a VLAN	Required Configure the untagged member ports and tagged member ports of the VLAN, or remove the specified ports from the VLAN.

2. VLAN configuration task list (approach II)

Task	Remarks
Creating VLANs	Required Create one or multiple VLANs.
Modifying ports	Required Configure ports as the untagged members or tagged members of VLANs, or remove ports from VLANs; configure the link type and PVID of the ports.

Creating VLANs

Select **Network** → **VLAN** from the navigation tree and click the **Create** tab to enter the page shown in a.

a. The Create tab

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove
-------------	---------------	-------------	--------	-------------	-------------	--------

Create:

VLAN IDs: Example:3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID	Description
<input type="text"/>	<input type="text"/> (1-32 Chars.)

2. Configuration items of creating VLANs

Item	Description
VLAN IDs	IDs of the VLANs to be created.
Modify the description of the selected VLAN	ID Select the ID of the VLAN whose description string is to be modified. Click the ID of the VLAN to be modified in the list in the middle of the page.
	Description Set the description string of the selected VLAN. By default, the description string of a VLAN is its VLAN ID, such as VLAN 0001 .

Return to [VLAN configuration task list \(approach I\)](#).

Return to [VLAN configuration task list \(approach II\)](#).

Selecting VLANs

Select **Network** → **VLAN** from the navigation tree. The **Select VLAN** tab is displayed by default for you to select VLANs, as shown in [a](#).

a. The Select VLAN tab

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove	
-------------	--------	-------------	--------	-------------	-------------	--------	--

VLAN range display: select an option to view all available VLANs or a subset of configured VLANs.

- Display all VLANs. Note: This option may reduce browser response time.
- Display a subset of all configured VLANs, example: 3,5-10.

Select

VLAN Summary

ID	Description	Untagged Membership	Tagged Membership

2. Configuration items of selecting VLANs

Item	Description
Display all VLANs	Select one of the two options:
Display a subnet of all configured VLANs	<ul style="list-style-type: none">• Display all VLANs—Display all configured VLANs.• Display a subnet of all configured VLANs—Type the VLAN IDs you want to display.

Return to [VLAN configuration task list \(approach I\)](#).

Modifying a VLAN

Select **Network** → **VLAN** from the navigation tree and click the **Modify VLAN** tab to enter the page shown in a.

a. The Modify VLAN tab

2. Configuration items of modifying a VLAN

Item	Description
Please select a VLAN to modify	Select the VLAN to be modified. Select a VLAN in the drop-down list. The VLANs available for selection are created first and then selected on the page for selecting VLANs.
Modify Description	Modify the description string of the selected VLAN. By default, the description string of a VLAN is its VLAN ID, such as VLAN 0001 .
Select membership type	Set the member type of the port to be modified in the VLAN. The options include: <ul style="list-style-type: none"> Untagged—Indicates that the port sends the traffic of the VLAN after removing the VLAN tag. Tagged—Indicates that the port sends the traffic of the VLAN without removing the VLAN tag. Not A Member—Remove the port from the VLAN.
Select ports to be modified and assigned to this VLAN	Select the ports to be modified in the selected VLAN. Click one or more ports you want to modify on the chassis front panel. If aggregate interfaces are configured on the device, the page displays a list of aggregate interfaces below the chassis front panel, and you can select aggregate interfaces from this list.

Return to [VLAN configuration task list \(approach I\)](#).

Modifying ports

Select **Network** → **VLAN** from the navigation tree and click the **Modify Port** tab to enter the page shown in a.

a. The Modify Port tab

2. Configuration items of modifying ports

Item	Description
Select Ports	<p>Select the ports to be modified.</p> <p>Click one or more ports you want to modify on the chassis front panel.</p> <p>If aggregate interfaces are configured on the device, the page displays a list of aggregate interfaces below the chassis front panel, and you can select aggregate interfaces from this list.</p>
Select membership type	<p>Set the member types of the selected ports to be modified in the specified VLANs.</p> <p>The options include:</p> <ul style="list-style-type: none"> Untagged—Assign the selected ports to the specified VLANs as untagged members. After that, the ports send the traffic of those VLANs after removing the VLAN tags. Tagged—Assign the selected ports to the specified VLANs as tagged members. After that, the ports send the traffic of those VLANs without removing the VLAN tags. Not A Member—Remove the selected ports from the specified VLANs.

Item	Description
VLAN IDs	Set the IDs of the VLANs that the selected ports are to be assigned to or removed from. This item is available when the Untagged , Tagged , or Not A Member option is selected in the Select membership type area.
Link Type	Set the link type of the selected ports, which can be access, hybrid, or trunk. This item is available when the Link Type option is selected in the Select membership type area.
PVID	Set the PVID of the selected ports. If you select Delete , you restore the PVID to VLAN 1.
Delete	This item is available when the PVID option is selected in the Select membership type area.

Return to [VLAN configuration task list \(approach II\)](#).

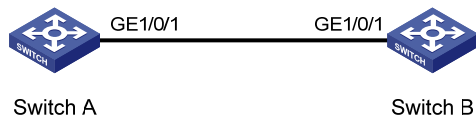
VLAN configuration example

Network requirements

As shown in a:

- Trunk port GigabitEthernet 1/0/1 of Switch A is connected to trunk port GigabitEthernet 1/0/1 of Switch B.
- The PVID of GigabitEthernet 1/0/1 is VLAN 100.
- GigabitEthernet 1/0/1 permits packets of VLAN 2, VLAN 6 through VLAN 50, and VLAN 100 to pass through.

a. Network diagram for VLAN configuration



Configuration procedure

Table 44 Configure Switch A

Configure GigabitEthernet 1/0/1 as a trunk port and configure VLAN 100 as its PVID.

Select **Device** → **Port Management** from the navigation tree and click the **Setup** tab to enter the page shown in b.

b. Configure GigabitEthernet 1/0/1 as a trunk port and its PVID as 100

Summary Detail **Setup**

Basic Configuration

Port State Speed Duplex

Link Type PVID 100 (1-4094)

Advanced Configuration

MDI Flow Control

Power Save Max MAC Count (0-8192)

Storm Suppression

Broadcast Suppression Multicast Suppression Unicast Suppression

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kpps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

HP V1910-16G Sw...

Select All Select None

Unit	Selected Ports
1	GE1/0/1

• It may take some time if you apply the above settings to multiple ports.

- Select **Trunk** in the **Link Type** drop-down list.
- Select the **PVID** option, and type **100** in the text box.
- Select GigabitEthernet 1/0/1 on the chassis front device panel.
- Click **Apply**.

Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100.

Select **Network** → **VLAN** from the navigation tree and click the **Create** tab to enter the page shown in c.

c. **Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100**

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove
-------------	---------------	-------------	--------	-------------	-------------	--------

Create:

VLAN IDs: Example: 3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID	Description
<input type="text"/>	<input type="text" value=""/>

(1-32 Chars.)

- Type VLAN IDs **2, 6-50, 100**.
 - Click **Create**.
- # Assign GigabitEthernet 1/0/1 to VLAN 100 as an untagged member.
- Click **Select VLAN** to enter the page for selecting VLANs, as shown in [d](#).

d. Set a VLAN range

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove	
-------------	--------	-------------	--------	-------------	-------------	--------	--

VLAN range display: select an option to view all available VLANs or a subset of configured VLANs.

- Display all VLANs. Note: This option may reduce browser response time.
- 1-100 Display a subset of all configured VLANs, example: 3,5-10.

Select

VLAN Summary

ID	Description	Untagged Membership	Tagged Membership

- Select the **Display a subnet of all configured VLANs** option and type **1-100** in the text box.
- Click **Select**.

Click **Modify VLAN** to enter the page for modifying the ports in a VLAN, as shown in e.

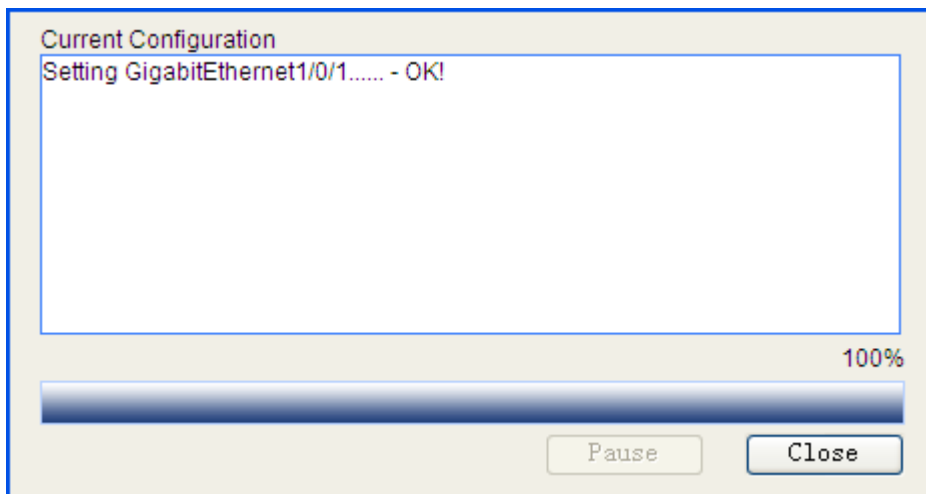
e. Assign GigabitEthernet 1/0/1 to VLAN 100 as an untagged member

The screenshot shows a configuration page with several sections:

- Navigation:** Select VLAN, Create, Port Detail, Detail, **Modify VLAN**, Modify Port, Remove.
- VLAN Selection:** "Please select a VLAN to modify:" dropdown menu with "100 - VLAN 0100" selected. "Modify Description (optional)" field with "VLAN 0100" and "(1-32 Chars.)" label. "Apply" button.
- Membership Type:** "Select membership type:" section with radio buttons for "Untagged" (selected), "Tagged", "Not A Member", and "Not available for selection".
- Port Selection:** "Select ports to be modified and assigned to this VLAN:" section. A port grid for "HP V1910-16G Sw..." with port 1 highlighted. "Select All" and "Select None" buttons. Note: "You can assign multiple ports in different membership types to this VLAN."
- Summary:** "Summary" section with "Untagged Membership" and "Tagged Membership" tabs. "GE1/0/1" is entered under "Untagged Membership". "Apply" and "Cancel" buttons.

- Select **100 – VLAN 0100** in the **Please select a VLAN to modify** drop-down list.
- Select the **Untagged** option in the **Select membership type** area.
- Select GigabitEthernet 1/0/1 on the chassis front device panel.
- Click **Apply**. A configuration progress dialog box appears, as shown in **f**.

f. Configuration progress dialog box



- After the configuration process is complete, click **Close**.

Assign GigabitEthernet 1/0/1 to VLAN 2 and VLANs 6 through 50 as a tagged member.

Click **Modify Port** to enter the page for modifying the VLANs to which a port belongs, as shown in g.

g. Assign GigabitEthernet 1/0/1 to VLAN 2 and VLANs 6 through 50 as a tagged member

- Select GigabitEthernet 1/0/1 on the chassis front device panel.
- Select the **Tagged** option in the **Select membership type** area.
- Type VLAN IDs **2, 6-50**.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close** in the dialog box.

Table 45 Configure Switch B

Configure Switch B as you configured Switch A.

Configuration guidelines

When configuring the VLAN function, follow these guidelines:

- As the default VLAN, VLAN 1 cannot be created or removed.
- You cannot create or remove VLANs reserved for special purposes.
- Dynamic VLANs cannot be removed on the page for removing VLANs.
- You cannot remove a VLAN that has referenced a QoS policy.
- To remove a remote probe VLAN for remote port mirroring, you must remove the remote probe VLAN configuration first.

VLAN interface configuration

NOTE:

For more information about VLANs, see the chapter “VLAN configuration.”

For hosts of different VLANs to communicate, you must use a router or Layer 3 switch to perform layer 3 forwarding. To achieve this, VLAN interfaces are used.

VLAN interfaces are virtual interfaces used for Layer 3 communication between different VLANs. They do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface. You can assign the VLAN interface an IP address and specify it as the gateway of the VLAN to forward the traffic destined for an IP subnet different from that of the VLAN.

Configuring VLAN interfaces

Configuration task list

Perform the tasks in 1 to configure a VLAN interface:

1. VLAN interface configuration task list

Task	Remarks
Creating a VLAN interface	Required Create a VLAN interface. You can select to assign an IPv4 address to the VLAN interface in this step or in a separate step. Before creating a VLAN interface for a VLAN, create the VLAN first (select Network → VLAN). For more information about the configuration procedure, see the chapter “VLAN configuration”.
Modifying a VLAN interface	Optional Assign an IPv4 address to the VLAN interface, and shut down or bring up the VLAN interface.

Creating a VLAN interface

Select **Network** → **VLAN Interface** from the navigation tree and click the **Create** tab to enter the page shown in a.

a. The Create tab

Summary	Create	Modify	Remove
---------	--------	--------	--------

Input a VLAN ID:

(1-4094)

Configure Primary IPv4 Address

DHCP BOOTP Manual

IPv4 Address: Mask Length: 24 (255.255.255.0)

Configure IPv6 Link Local Address

Auto Manual

IPv6 Address:

2. Configuration items of creating a VLAN interface

Item	Description	
Input a VLAN ID:	Input the ID of the VLAN interface to be created. Before creating a VLAN interface, make sure that the corresponding VLAN exists.	
Configure Primary IPv4 Address	DHCP	Configure the way in which the VLAN interface obtains an IPv4 address.
	BOOTP	Allow the VLAN interface to automatically obtain an IP address by selecting the DHCP or BOOTP option, or manually assign the VLAN interface an IP address by selecting the Manual option.
	Manual	
	IPv4 Address	Configure an IPv4 address for the VLAN interface. This option is available after you select the Manual option.
Mask Length	Select the subnet mask length. This option is available after you select the Manual option.	

Return to [VLAN interface configuration task list](#).

Modifying a VLAN interface

NOTE:

After you modify the IPv4 address for a selected VLAN interface on the page for modifying VLAN interfaces, click the **Apply** button to submit the modification.

After you change the IP address of the VLAN interface you are using to log in to the device, you will be disconnected from the device. You can use the changed IP address to re-log in.

Select **Network** → **VLAN Interface** from the navigation tree and click the **Modify** tab to enter the page shown in a.

a. The Modify tab

Summary
Create
Modify
Remove

Select VLAN Interface 999 ▼

Modify IPv4 Address

Modify Primary IP And Status

DHCP
 BOOTP
 Manual

Admin Status Up ▼

Apply

Modify IPv6 Address

Modify IPv6 Link Local Address And Status

Auto
 Manual

Admin Status Up ▼

Apply

Add IPv6 Unicast Address

64 ▼

EUI-64

Apply

IPv6 Address

2. Configuration items of modifying a VLAN interface

Item	Description
Select VLAN Interface	Select the VLAN interface to be configured. The VLAN interfaces available for selection in the drop-down list are those created on the page for creating VLAN interfaces.
Modify IPv4 Address	Configure the way in which the VLAN interface obtains an IPv4 address. Allow the VLAN interface to obtain an IP address automatically by selecting the DHCP or BOOTP option, or manually assign the VLAN interface an IP address by selecting the Manual option.

Item	Description
Admin Status	<p>Select Up or Down in the Admin Status drop-down list to bring up or shut down the selected VLAN interface.</p> <p>To restore a failed VLAN interface, you can shut down and then bring up the VLAN interface.</p> <p>By default, a VLAN interface is down if all Ethernet ports in the VLAN are down, and is up if one or more Ethernet ports in the VLAN are up.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> • The current VLAN interface state in the Modify IPv4 Address area changes if the VLAN interface state is modified in the Admin Status drop-down list. • The state of each port in the VLAN is independent of the VLAN interface state.

Return to [VLAN interface configuration task list](#).

Voice VLAN configuration

A voice VLAN is configured especially for voice traffic. After assigning the ports connecting to voice devices to a voice VLAN, the system automatically configures quality of service (QoS) parameters for voice traffic, improving the transmission priority of voice traffic and ensuring voice quality.

OUI addresses

A device determines whether a received packet is a voice packet by checking its source MAC address. A packet whose source MAC address complies with the voice device's Organizationally Unique Identifier (OUI) address is regarded as voice traffic.

You can configure the OUI addresses of a device in advance or use the default OUI addresses. 1 lists the default OUI address for each vendor's devices.

1. The default OUI addresses of different vendors

Number	OUI Address	Vendor
1	0001-E300-0000	Siemens phone
2	0003-6B00-0000	Cisco phone
3	0004-0D00-0000	Avaya phone
4	00D0-1E00-0000	Pingtel phone
5	0060-B900-0000	Philips/NEC phone
6	00E0-7500-0000	Polycom phone
7	00E0-BB00-0000	3Com phone

NOTE:

In general, as the first 24 bits of a MAC address (in binary format), an OUI address is a globally unique identifier assigned to a vendor by the IEEE. OUI addresses mentioned in this document, however, are different from those commonly used. In this document, OUI addresses are used by the system to determine whether a received packet is a voice packet. They are the results of the AND operation of a MAC address and a mask. For more information, see ["Adding OUI addresses to the OUI list"](#).

You can manually remove the default OUI address of a device and then add new ones.

Voice VLAN assignment modes

A port can be assigned to a voice VLAN in one of the following modes:

- In automatic mode, the system matches the source MAC addresses carried in the untagged packets sent when an IP phone is powered on against the device's OUI addresses. If a match is found, the system automatically assigns the receiving port to a voice VLAN, issues ACL rules and configures the packet precedence. You can configure voice VLAN aging time on the device. The system will remove

a port from the voice VLAN if no packet is received from the port during the aging time. Assigning ports to and removing ports from a voice VLAN are automatically performed.

- In manual mode, you need to manually assign an IP phone accessing port to a voice VLAN. Then, the system matches the source MAC addresses carried in the packets against the device's OUI addresses. If a match is found, the system issues ACL rules and configures the packet precedence. In this mode, assigning ports to and removing ports from a voice VLAN are performed manually.

Both modes forward tagged packets according to their tags.

1 lists the relationships between the voice assignment VLAN mode, the voice traffic type of an IP phone, and the port link type.

1. Co-relation

Voice VLAN assignment mode	Voice traffic type	Port link type		
		Access	Trunk	Hybrid
Automatic mode	Tagged voice traffic	Not supported	Supported, but you must ensure that the PVID of the port has been created and is not the voice VLAN and the traffic of the PVID can pass through the port.	Supported, but you must ensure that the PVID of the port has been created and is not the voice VLAN and the traffic of the PVID can pass through the port tagged.
	Untagged voice traffic	Not supported	Not supported	Not supported
Manual mode	Tagged voice traffic	Not supported	Supported, but you must ensure that the PVID of the port has been created and is not the voice VLAN and the traffic of the PVID can pass through the port.	Supported, but you must ensure that the PVID of the port has been created and is not the voice VLAN and the traffic of the voice VLAN can pass through the port tagged.
	Untagged voice traffic	Supported, but you must configure the PVID of the port as the voice VLAN.	Supported, but you must configure the PVID of the port as the voice VLAN and configure the port to allow the traffic of the voice VLAN to pass through.	Supported, but you must configure the PVID of the port as the voice VLAN and configure the port to allow the traffic of the voice VLAN to pass through untagged.

NOTE:

If an IP phone sends tagged voice traffic and its accessing port is configured with 802.1X authentication and guest VLAN, you must assign different VLAN IDs for the voice VLAN, the port VLAN ID (PVID) of the accessing port, and the 802.1X guest VLAN.

If an IP phone sends untagged voice traffic, to implement the voice VLAN feature, you must configure the PVID of the IP phone's accessing port as the voice VLAN. As a result, 802.1X authentication cannot be implemented.

Security mode and normal mode of voice VLANs

Depending on their inbound packet filtering mechanisms, voice VLAN-enabled port can operate in the following modes:

- **Normal mode:** In this mode, voice VLAN-enabled ports receive packets carrying the voice VLAN tag and forward packets in the voice VLAN without checking their source MAC addresses against the OUI addresses configured for the device. If the PVID of the port is the voice VLAN and the port works in manual VLAN assignment mode, the port forwards all received untagged packets in the voice VLAN. In normal mode, the voice VLANs are vulnerable to traffic attacks. Vicious users may forge a large amount of voice packets and send them to the device to consume the voice VLAN bandwidth, affecting normal voice communication.
- **Security mode:** In this mode, only voice packets whose source MAC addresses match the recognizable OUI addresses can pass through the voice VLAN-enabled inbound port, but all other packets are dropped.

In a safe network, you can configure the voice VLANs to operate in normal mode, reducing the consumption of system resources due to source MAC addresses checking.

HP does not recommend you transmit both voice traffic and non-voice traffic in a voice VLAN. If you have to, ensure that the voice VLAN security mode is disabled.

1. How a voice VLAN-enable port processes packets in security/normal mode

Voice VLAN mode	Packet type	Packet processing mode
Security mode	Untagged packets	If the source MAC address of a packet matches an OUI address configured for the device, it is forwarded in the voice VLAN; otherwise, it is dropped.
	Packets carrying the voice VLAN tag	
	Packets carrying other tags	Forwarded or dropped depending on whether the port allows packets of these VLANs to pass through
Normal mode	Untagged packets	The port does not check the source MAC addresses of inbound packets. In this way, both voice traffic and non-voice traffic can be transmitted in the voice VLAN.
	Packets carrying the voice VLAN tag	
	Packets carrying other tags	Forwarded or dropped depending on whether the port allows packets of these VLANs to pass through

Configuring the voice VLAN

Configuration task list

Before configuring the voice VLAN feature, you must create the corresponding VLAN and configure the link type of each port to be assigned to the VLAN. VLAN 1 is the default VLAN, and you cannot create it or configure it as a voice VLAN. For more information about port link types, see the chapter “Port management configuration”.

Configuring voice VLAN on a port in automatic voice VLAN assignment mode

Perform the tasks described in 1 to configure the voice VLAN function on a port working in automatic voice VLAN assignment mode.

1. Voice VLAN configuration task list for a port in automatic voice VLAN assignment mode

Task	Remarks
Configuring voice VLAN globally	Optional Configure the voice VLAN to operate in security mode and configure the aging timer.
Configuring voice VLAN on a port	Required Configure the voice VLAN assignment mode of a port as automatic and enable the voice VLAN function on the port. By default, the voice VLAN assignment mode of a port is automatic, and the voice VLAN function is disabled on a port.
Adding OUI addresses to the OUI list	Optional You can configure up to 16 OUI addresses. By default, the system is configured with seven OUI addresses, as shown in 1.

Configuring voice VLAN on a port working in manual voice VLAN assignment mode

Perform the tasks described in 1 to configure the voice VLAN function on a port working in manual voice VLAN assignment mode.

1. Configuration task list for a port in manual voice VLAN assignment mode

Task	Remarks
Configuring voice VLAN globally	Optional Configure the voice VLAN to operate in security mode and configure the aging timer.
Assigning the port to the voice VLAN	Required After an access port is assigned to the voice VLAN, the voice VLAN automatically becomes the PVID of the access port. For more information, see the chapter "VLAN configuration".
Configuring the voice VLAN as the PVID of a hybrid or trunk port	Optional This task is required if the incoming voice traffic is untagged and the link type of the receiving port is trunk or hybrid. If the incoming voice traffic is tagged, do not perform this task. For more information, see the chapter "Port management configuration".
Configuring voice VLAN on a port	Required Configure the voice VLAN assignment mode of a port as manual and enable the voice VLAN function on the port. By default, the voice VLAN assignment mode of a port is automatic, and the voice VLAN function is disabled on a port.

Task	Remarks
Adding OUI addresses to the OUI list	Optional You can configure up to 16 OUI addresses. By default, the system is configured with seven OUI addresses, as shown in 1 .

Configuring voice VLAN globally

Select **Network** → **Voice VLAN** from the navigation tree, and click the **Setup** tab to enter the page shown in [a](#).

a. Configure voice VLAN

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove	
Voice VLAN security: <input type="text" value="Enable"/>						
Voice VLAN aging time: <input type="text" value="1440"/> minutes (5-43200, Default = 1440)						
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>						

2. Global voice VLAN configuration items

Item	Description
Voice VLAN security	Select Enable or Disable in the drop-down list to enable or disable the voice VLAN security mode. By default, the voice VLANs operate in security mode.
Voice VLAN aging time	Set the voice VLAN aging timer. The voice VLAN aging timer applies only to a port in automatic voice VLAN assignment mode. The voice VLAN aging timer starts as soon as the port is assigned to the voice VLAN. If no voice packet has been received before the timer expires, the port is removed from the voice VLAN.

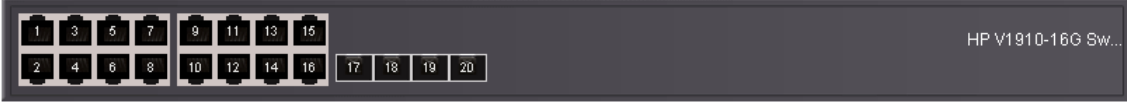
Return to [Configuring voice VLAN on a port in automatic voice VLAN assignment mode](#).

Return to [Configuring voice VLAN on a port working in manual voice VLAN assignment mode](#).

Configuring voice VLAN on a port

Select **Network** → **Voice VLAN** from the navigation tree, and click the **Port Setup** tab to enter the page shown in [a](#).

a. Configure voice VLAN on a port

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove
Voice VLAN port mode: <input type="text" value="No Change"/>					
Voice VLAN port state: <input type="text" value="No Change"/>					
Voice VLAN ID: <input type="text"/> (2-4094)					
Select ports: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">  </div>					
<input type="button" value="Select All"/> <input type="button" value="Select None"/>					
Ports selected for voice VLAN: <div style="border: 1px solid gray; height: 30px; margin: 5px 0;"></div>					
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>					

2. Configuration items of configuring voice VLAN for a port

Item	Description
Voice VLAN port mode	Set the voice VLAN assignment mode of a port: <ul style="list-style-type: none"> • Auto—Indicates the automatic voice VLAN assignment mode. • Manual—Indicates the manual voice VLAN assignment mode.
Voice VLAN port state	Select Enable or Disable in the drop-down list to enable or disable the voice VLAN function on the port.
Voice VLAN ID	Set the voice VLAN ID. This option is available when the voice VLAN port state is set to Enable . ⓘ IMPORTANT: The device supports only one voice VLAN. Only an existing static VLAN can be configured as the voice VLAN.
Select ports	Select the port on the chassis front panel. You can select multiple ports to configure them in bulk. The interface numbers of the selected ports will be displayed in the Ports selected for voice VLAN text box. ⓘ IMPORTANT: To set the voice VLAN assignment mode of a port to automatic, ensure that the link type of the port is trunk or hybrid, and that the port does not belong to the voice VLAN.

Return to [Configuring voice VLAN on a port in automatic voice VLAN assignment mode.](#)

Return to [Configuring voice VLAN on a port working in manual voice VLAN assignment mode.](#)

Adding OUI addresses to the OUI list

Select **Network** → **Voice VLAN** from the navigation tree and click the **OUI Add** tab to enter the page shown in a.

a. Add OUI addresses to the OUI list

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove
---------	-------	------------	-------------	---------	------------

Specify an OUI and click Apply to add it to the list. There can be 16 entries at most.

OUI Address:

Mask:

Description:

OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0005-2100-0000	ffff-ff00-0000	Phone A
0005-2200-0000	ffff-ff00-0000	Phone B
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

2. OUI list configuration items

Item	Description
OUI Address	Set the source MAC address of voice traffic.
Mask	Set the mask length of the source MAC address.
Description	Set the description of the OUI address entry.

Return to [Configuring voice VLAN on a port in automatic voice VLAN assignment mode.](#)

Return to [Configuring voice VLAN on a port working in manual voice VLAN assignment mode.](#)

Voice VLAN configuration examples

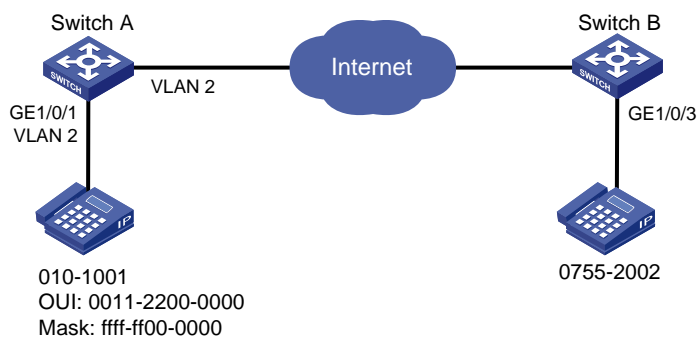
Configuring voice VLAN on a port in automatic voice VLAN assignment mode

Network requirements

As shown in [a](#),

- Configure VLAN 2 as the voice VLAN allowing only voice traffic to pass through.
- The IP phone connected to hybrid port GigabitEthernet 1/0/1 sends untagged voice traffic.
- GigabitEthernet 1/0/1 operates in automatic VLAN assignment mode. Set the voice VLAN aging timer to 30 minutes.
- Configure GigabitEthernet 1/0/1 to allow voice packets whose source MAC addresses match the OUI addresses specified by OUI address 0011-2200-0000 and mask FFFF-FF00-0000. The description of the OUI address entry is **test**.

[a](#). Network diagram for automatic voice VLAN assignment mode configuration



Configuration procedure

Create VLAN 2.

- Select **Network** → **VLAN** from the navigation tree, and click the **Create** tab to enter the page shown in [a](#).

a. **Create VLAN 2**

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove
-------------	---------------	-------------	--------	-------------	-------------	--------

Create:

VLAN IDs:	<input type="text" value="2"/>	Example:3, 5-10
		<input type="button" value="Create"/>

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID	Description
<input type="text"/>	<input type="text" value=""/>
	(1-32 Chars.)
	<input type="button" value="Apply"/>

- Type VLAN ID 2.
- Click **Create**.

Configure GigabitEthernet 1/0/1 as a hybrid port.

- Select **Device** → **Port Management** from the navigation tree, and click the **Setup** tab to enter the page shown in [b](#).

b. Configure GigabitEthernet 1/0/1 as a hybrid port

Summary Detail **Setup**

Basic Configuration

Port State Speed Duplex

Link Type PVID (1-4094)

Advanced Configuration

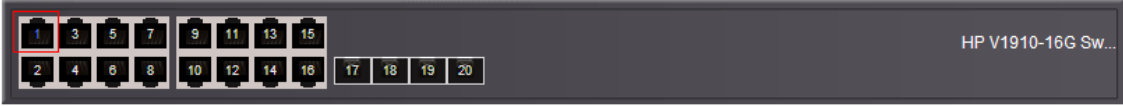
MDI Flow Control

Power Save Max MAC Count (0-8192)

Storm Suppression

Broadcast Suppression Multicast Suppression Unicast Suppression

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kpps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

 HP V1910-16G Sw...

Select All Select None

Unit Selected Ports

1 GE1/0/1

• It may take some time if you apply the above settings to multiple ports.

- Select **Hybrid** from the **Link Type** drop-down list.
- Select GigabitEthernet 1/0/1 from the chassis front panel.
- Click **Apply**.

Configure the voice VLAN function globally.

- Select **Network** → **Voice VLAN** from the navigation tree and click the **Setup** tab to enter the page shown in c.

c. Configure the voice VLAN function globally

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove
---------	-------	------------	-------------	---------	------------

Voice VLAN security:

Voice VLAN aging time: minutes (5-43200, Default = 1440)

- Select **Enable** in the **Voice VLAN security** drop-down list. You can skip this step, because the voice VLAN security mode is enabled by default.
- Set the voice VLAN aging timer to 30 minutes.
- Click **Apply**.

Configure voice VLAN on GigabitEthernet 1/0/1.

- Click the **Port Setup** tab to enter the page shown in d.

d. Configure voice VLAN on GigabitEthernet 1/0/1

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove
---------	-------	------------	-------------	---------	------------

Voice VLAN port mode:

Voice VLAN port state:

Voice VLAN ID : (2-4094)

Select ports:

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	3	5	7	9	11	13	15												
2	4	6	8	10	12	14	16	17	18	19	20								

Ports selected for voice VLAN:

- Select **Auto** in the **Voice VLAN port mode** drop-down list.
- Select **Enable** in the **Voice VLAN port state** drop-down list.
- Type voice VLAN ID 2.
- Select GigabitEthernet 1/0/1 on the chassis front panel.
- Click **Apply**.

Add OUI addresses to the OUI list.

- Click the **OUI Add** tab to enter the page shown in e.

e. Add OUI addresses to the OUI list

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove
---------	-------	------------	-------------	---------	------------

Specify an OUI and click Apply to add it to the list. There can be 16 entries at most.

OUI Address:	<input type="text" value="0011-2200-0000"/>
Mask:	<input type="text" value="FFFF-FF00-0000"/> ▼
Description:	<input type="text" value="test"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

- Type OUI address **0011-2200-0000**.
- Select **FFFF-FF00-0000** in the **Mask** drop-down list.
- Type description string **test**.
- Click **Apply**.

Verify the configuration

- When the configurations are completed, the **OUI Summary** tab is displayed by default, as shown in **a**. You can view information about the newly-added OUI address.

a. Current OUI list of the device

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove
---------	-------	------------	-------------	---------	------------

OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0011-2200-0000	ffff-ff00-0000	test
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

- Click the **Summary** tab to enter the page shown in **b**, where you can view the current voice VLAN information.

b. Current voice VLAN information

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove	
Voice VLAN security:			Enabled			
Voice VLAN aging time:			30 minutes			
Maximum of voice VLANs :			1			
Current number of voice VLANs :			1			

Ports enabled for voice VLAN:

Port Name	Voice VLAN ID	Mode
GigabitEthernet1/0/1	2	Auto

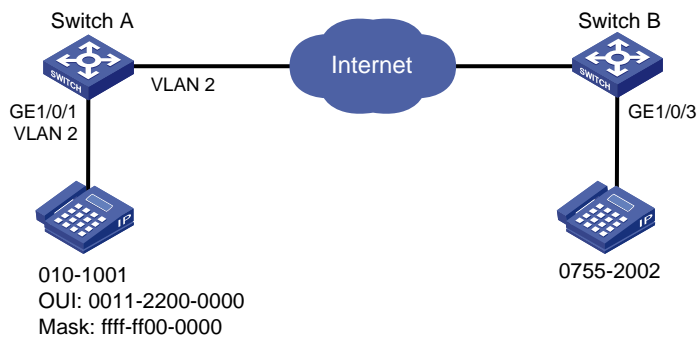
Configuring a voice VLAN on a port in manual voice VLAN assignment mode

Network requirements

As shown in a,

- Configure VLAN 2 as a voice VLAN that carries only voice traffic.
- The IP phone connected to hybrid port GigabitEthernet 1/0/1 sends untagged voice traffic.
- GigabitEthernet 1/0/1 operates in manual voice VLAN assignment mode and allows voice packets whose source MAC addresses match the OUI addresses specified by OUI address 0011-2200-0000 and mask FFFF-FF00-0000 to pass through. The description of the OUI address entry is **test**.

a. Network diagram for manual voice VLAN assignment mode configuration



Configuration procedure

Create VLAN 2.

- Select **Network** → **VLAN** from the navigation tree, and click the **Create** tab to enter the page shown in a.

a. Create VLAN 2

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove
-------------	---------------	-------------	--------	-------------	-------------	--------

Create:

VLAN IDs: Example:3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID	Description
<input type="text"/>	<input type="text" value=""/> (1-32 Chars.)

- Type VLAN ID 2.
- Click **Create**.

Configure GigabitEthernet 1/0/1 as a hybrid port and configure its PVID as VLAN 2.

- Select **Device** → **Port Management** from the navigation tree, and click the **Setup** tab to enter the page shown in b.

b. Configure GigabitEthernet 1/0/1 as a hybrid port

Summary Detail Setup

Basic Configuration

Port State No Change Speed No Change Duplex No Change

Link Type Hybrid PVID 2 (1-4094)

Advanced Configuration

MDI No Change Flow Control No Change

Power Save No Change Max MAC Count No Change (0-8192)

Storm Suppression

Broadcast Suppression No Change Multicast Suppression No Change Unicast Suppression No Change

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kpps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

HP V1910-16G Sw...

Select All Select None

Unit	Selected Ports
1	GE1/0/1

• It may take some time if you apply the above settings to multiple ports.

Apply Cancel

- Select **Hybrid** from the **Link Type** drop-down list.
- Select the **PVID** option and type **2** in the text box.
- Select GigabitEthernet 1/0/1 from the chassis front panel.
- Click **Apply**.

Assign GigabitEthernet 1/0/1 to VLAN 2 as an untagged member.

- Select **Network** → **VLAN** from the navigation tree, and click the **Modify Port** tab to enter the page shown in c.

c. Assign GigabitEthernet 1/0/1 to VLAN 2 as an untagged member

The screenshot shows a web-based configuration interface for a network device. At the top, there is a navigation bar with tabs: Select VLAN, Create, Port Detail, Detail, Modify VLAN, Modify Port (selected), and Remove. Below the navigation bar, the 'Select Ports' section displays a grid of port numbers from 1 to 20. Port 1 is highlighted with a red box. To the right of the grid, the text 'HP V1910-16G Sw...' is visible. Below the grid are 'Select All' and 'Select None' buttons, and a 'Not available for selection' indicator. The 'Select membership type:' section has five radio buttons: 'Untagged' (selected and highlighted with a red box), 'Tagged', 'Not A Member', 'Link Type', and 'PVID'. The 'Enter VLAN IDs to which the port is to be assigned:' section has a text input field containing '2' (highlighted with a red box) and an 'Example: 1,3,5-10' label. The 'Selected ports:' section shows a list box containing 'Untagged Membership' and 'GE1/0/1' (highlighted with a red box). At the bottom right, there are 'Apply' and 'Cancel' buttons, with 'Apply' highlighted by a red box.

- Select GigabitEthernet 1/0/1 from the chassis front panel.
- Select the **Untagged** option.
- Type VLAN ID 2.
- Click **Apply**. A configuration progress dialog box appears, as shown in d.

d. Configuration progress dialog box

The screenshot shows a configuration progress dialog box titled 'Current Configuration'. The main text area contains the message 'Setting GigabitEthernet1/0/1..... - OK!'. At the bottom right, a progress bar is shown at 100%. Below the progress bar are 'Pause' and 'Close' buttons.

- After the configuration process is complete, click **Close**.

Configure voice VLAN on GigabitEthernet 1/0/1.

- Select **Network** → **Voice VLAN** from the navigation tree, and click the **Port Setup** tab to enter the page shown in e.

e. **Configure voice VLAN on GigabitEthernet 1/0/1**

The screenshot shows the configuration page for Voice VLAN on GigabitEthernet 1/0/1. The 'Port Setup' tab is selected. The configuration fields are:

- Voice VLAN port mode: Manual
- Voice VLAN port state: Enable
- Voice VLAN ID: 2 (range 2-4094)

 Below these fields is a 'Select ports:' section with a grid of 20 ports. Port 1 is highlighted. Below the grid are 'Select All' and 'Select None' buttons. A list titled 'Ports selected for voice VLAN:' contains 'GE1/0/1'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

- Select **Manual** in the **Voice VLAN port mode** drop-down list.
- Select **Enable** in the **Voice VLAN port state** drop-down list.
- Type voice VLAN ID 2.
- Select GigabitEthernet 1/0/1 on the chassis front panel.
- Click **Apply**.

Add OUI addresses to the OUI list.

- Click the **OUI Add** tab to enter the page shown in f.

f. Add OUI addresses to the OUI list

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove
---------	-------	------------	-------------	---------	------------

Specify an OUI and click Apply to add it to the list. There can be 16 entries at most.

OUI Address:	<input type="text" value="0011-2200-0000"/>
Mask:	<input type="text" value="FFFF-FF00-0000"/> ▼
Description:	<input type="text" value="test"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

- Type OUI address **0011-2200-0000**.
- Select **FFFF-FF00-0000** from the **Mask** drop-down list.
- Type description string **test**.
- Click **Apply**.

Verify the configuration

- When the configurations are completed, the **OUI Summary** tab is displayed by default, as shown in **a**. You can view information about the newly-added OUI address.

a. Current OUI list of the device

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove
---------	-------	------------	-------------	---------	------------

OUI Address	Mask	Description
0001-e300-0000	ffff-ff00-0000	Siemens phone
0003-6b00-0000	ffff-ff00-0000	Cisco phone
0004-0d00-0000	ffff-ff00-0000	Avaya phone
0011-2200-0000	ffff-ff00-0000	test
0060-b900-0000	ffff-ff00-0000	Philips/NEC phone
00d0-1e00-0000	ffff-ff00-0000	Pingtel phone
00e0-7500-0000	ffff-ff00-0000	Polycom phone
00e0-bb00-0000	ffff-ff00-0000	3com phone

- Click the **Summary** tab to enter the page shown in **b**, where you can view the current voice VLAN information.

b. Current voice VLAN information

Summary	Setup	Port Setup	OUI Summary	OUI Add	OUI Remove	
Voice VLAN security:			Enabled			
Voice VLAN aging time:			1440 minutes			
Maximum of voice VLANs :			1			
Current number of voice VLANs :			1			

Ports enabled for voice VLAN:

Port Name	Voice VLAN ID	Mode
GigabitEthernet1/0/1	2	Manual

Configuration guidelines

When configuring the voice VLAN function, follow these guidelines:

- To remove a VLAN functioning as a voice VLAN, disable its voice VLAN function first.
- In automatic voice VLAN assignment mode, a hybrid port can process only tagged voice traffic. However, the protocol-based VLAN function requires hybrid ports to process untagged traffic. Therefore, if a VLAN is configured as the voice VLAN and a protocol-based VLAN at the same time, the protocol-based VLAN cannot be associated with the port.
- Only one VLAN is supported and only one existing static VLAN can be configured as the voice VLAN.
- If Link Aggregation Control Protocol (LACP) is enabled on a port, the voice VLAN function cannot be enabled on it.
- After you assign a port working in manual voice VLAN assignment mode to the voice VLAN, the voice VLAN takes effect.

MAC address configuration

NOTE:

The MAC address table can contain only Layer 2 Ethernet ports.

This manual covers only the management of static and dynamic MAC address entries, not multicast MAC address entries.

An Ethernet device uses a MAC address table for forwarding frames through unicast instead of broadcast. This table describes from which port a MAC address (or host) can be reached. The entries in the MAC address table come from two sources: automatically learned by the device and manually added by the administrator. Static entries never age out, but dynamic entries, which are whether manually configured or dynamically learned, will age out.

The device can automatically populate its MAC address table by learning the source MAC addresses of incoming frames on each port.

When a frame arrives at a port, Port A for example, the device performs the following tasks:

Table 46 Checks the source MAC address (MAC-SOURCE for example) of the frame.

Table 47 Looks up the source MAC address in the MAC address table.

If an entry is found, the device updates the entry.

If no entry is found, the device adds an entry for MAC-SOURCE and Port A.

After learning the source MAC address, when the device receives a frame destined for MAC-SOURCE, the device finds the MAC-SOURCE entry in the MAC address table and forwards the frame out port A.

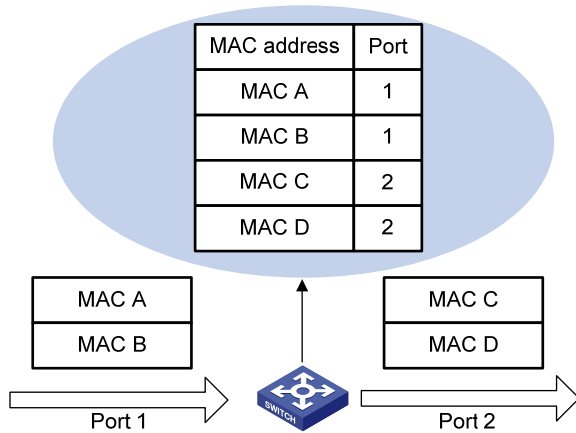
NOTE:

Dynamically learned MAC addresses cannot overwrite static MAC address entries, but the latter can overwrite the former.

When forwarding a frame, the device adopts the following two forwarding modes based on the MAC address table:

- Unicast mode: If an entry is available for the destination MAC address, the device forwards the frame out the outgoing interface indicated by the MAC address table entry.
- Broadcast mode: If the device receives a frame with an all-ones destination address, or no entry is available for the destination MAC address, the device broadcasts the frame to all the interfaces except the receiving interface.

b. MAC address table of the device



Configuring MAC addresses

You can configure and display MAC address entries and set the MAC address entry aging time.

Configuring a MAC address entry

Select **Network** → **MAC** from the navigation tree. The system automatically displays the **MAC** tab, which shows all the MAC address entries on the device, as shown in [a](#).

a. The MAC tab

MAC Setup

Search Item: MAC Keywords: Search

<input type="checkbox"/>	MAC	VLAN ID	Type	Port	Operation
<input type="checkbox"/>	000d-56fb-3880	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	000d-88f8-4e71	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	000f-cb00-5601	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	000f-e200-0144	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	000f-e207-f2e0	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	000f-e218-d0d1	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	0015-e943-712f	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	0015-e943-7326	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	0022-3377-998c	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	00e0-4c3d-35d7	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	00e0-fc00-000b	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	00e0-fc00-004f	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	00e0-fc00-3963	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	00e0-fc00-5503	1	Learned	GigabitEthernet1/0/15	
<input type="checkbox"/>	00e0-fc00-5544	1	Learned	GigabitEthernet1/0/15	

24 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Add Refresh Delete Selected

Click **Add** in the bottom to enter the page as shown in b.

b. Create a MAC address entry

MAC Setup

Add MAC

MAC: *(Example: 0010-dc28-a4e9)

Type: static

VLAN: 1

Port: GigabitEthernet1/0/1

Items marked with an asterisk(*) are required

Apply Cancel

2. Configuration items of creating a MAC address entry

Item	Description
MAC	Set the MAC address to be added.
Type	<p>Set the type of the MAC address entry:</p> <ul style="list-style-type: none">• Static—Static MAC address entries that never age out.• Dynamic—Dynamic MAC address entries that will age out.• Blackhole—Blackhole MAC address entries that never age out. <p>! IMPORTANT:</p> <p>The tab displays the following types of the MAC address entries:</p> <ul style="list-style-type: none">• Config static—Static MAC address entries manually configured.• Config dynamic—Dynamic MAC address entries manually configured.• Blackhole—Blackhole MAC address entries.• Learned—Dynamic MAC address entries learned by the device.• Other—Other types of MAC address entries.
VLAN	Set the ID of the VLAN to which the MAC address belongs.
Port	Set the port to which the MAC address belongs.

Setting the aging time of MAC address entries

Select **Network** → **MAC** from the navigation tree, and click the **Setup** tab to enter the page shown in a.

a. Set the aging time for MAC address entries

The screenshot shows the configuration page for MAC address entries. At the top, there are two tabs: 'MAC' and 'Setup'. The 'Setup' tab is active. Below the tabs, the page title is 'Set mac-address aging time'. There are two radio button options: 'No-aging' and 'Aging Time'. The 'Aging Time' option is selected. To the right of the 'Aging Time' option, there is a text input field containing the value '300', followed by the text 'seconds(10-630, Default = 300)'. At the bottom right of the page, there is an 'Apply' button.

2. Configuration items of setting the aging time for a MAC address entry

Item	Description
No-aging	Specify that the MAC address entry never ages out.
Aging time	Set the aging time for the MAC address entry.

MAC address configuration example

Network requirements

Use the web-based NMS to configure the MAC address table of the device. It is required to add a static MAC address 00e0-fc35-dc71 under GigabitEthernet 1/0/1 in VLAN 1.

Configuration procedure

Create a static MAC address entry.

Select **Network** → **MAC** from the navigation tree to enter the **MAC** tab, and then click **Add**. The page shown in [a](#) appears.

a. Create a static MAC address entry

The screenshot shows a web-based configuration interface for MAC addresses. At the top, there are two tabs: 'MAC' and 'Setup'. Below the tabs is a section titled 'Add MAC'. This section contains four input fields: 'MAC' with the value '00e0-fc35-dc71' and a note '(Example: 0010-dc28-a4e9)', 'Type' with a dropdown menu set to 'static', 'VLAN' with a dropdown menu set to '1', and 'Port' with a dropdown menu set to 'GigabitEthernet1/0/1'. Below these fields is a note: 'Items marked with an asterisk(*) are required'. At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

- Type MAC address **00e0-fc35-dc71**.
- Select **static** in the **Type** drop-down list.
- Select **1** in the **VLAN** drop-down list.
- Select **GigabitEthernet1/0/1** in the **Port** drop-down list.
- Click **Apply**.

MSTP configuration

As a Layer 2 management protocol, the Spanning Tree Protocol (STP) eliminates Layer 2 loops by selectively blocking redundant links in a network, and also allows for link redundancy.

Recent versions of STP include Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). This chapter describes the characteristics of STP, RSTP, MSTP, and the relationship among them.

STP

STP was developed based on the 802.1d standard of IEEE to eliminate loops at the data link layer in a local area network (LAN). Networks often have redundant links as backups in case of failures, but loops are a very serious problem. Devices running STP detect loops in the network by exchanging information with one another, and eliminate loops by selectively blocking certain ports to prune the loop structure into a loop-free tree structure. This avoids proliferation and infinite cycling of packets that would occur in a loop network and prevents decreased device performance caused by receiving duplicate packets.

In the narrow sense, STP refers to the IEEE 802.1d STP. In the broad sense, STP refers to the IEEE 802.1d STP and various enhanced spanning tree protocols derived from that protocol.

STP protocol packets

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP-enabled network devices exchange BPDUs to establish a spanning tree. BPDUs contain sufficient information for the network devices to complete spanning tree calculation.

STP uses the following types of BPDUs:

- Configuration BPDUs, used for calculating a spanning tree and maintaining the spanning tree topology.
- Topology change notification (TCN) BPDUs, which notify network devices of network topology changes.

Basic concepts in STP

Root bridge

A tree network must have a root bridge.

There is only one root bridge in the entire network. The root bridge is not permanent, but can change with changes of the network topology.

Upon initialization of a network, each device generates and periodically sends out configuration BPDUs with itself as the root bridge. After network convergence, only the root bridge generates and periodically sends out configuration BPDUs. The other devices only forward the BPDUs.

Root port

On a non-root bridge, the port nearest to the root bridge is the root port. The root port communicates with the root bridge. Each non-root bridge has only one root port. The root bridge has no root port.

Designated bridge and designated port

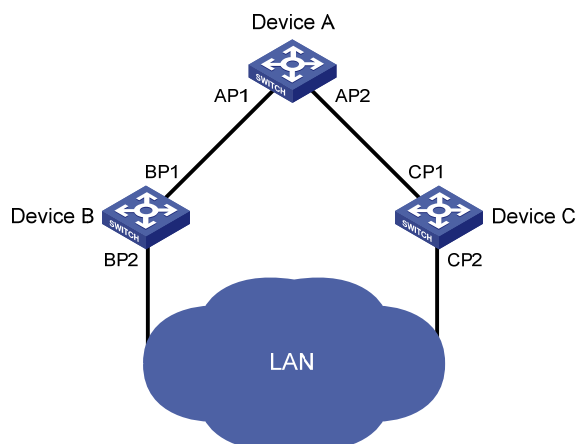
1. Description of designated bridges and designated ports

Classification	Designated bridge	Designated port
For a device	A device directly connected with the local device and responsible for forwarding BPDUs to the local device	The port through which the designated bridge forwards BPDUs to this device
For a LAN	The device responsible for forwarding BPDUs to this LAN segment	The port through which the designated bridge forwards BPDUs to this LAN segment

As shown in a, AP1 and AP2, BP1 and BP2, and CP1 and CP2 are ports on Device A, Device B, and Device C respectively.

- If Device A forwards BPDUs to Device B through AP1, the designated bridge for Device B is Device A, and the designated port of Device B is port AP1 on Device A.
- Two devices are connected to the LAN: Device B and Device C. If Device B forwards BPDUs to the LAN, the designated bridge for the LAN is Device B, and the designated port for the LAN is the port BP2 on Device B.

a. A schematic diagram of designated bridges and designated ports



Path cost

Path cost is a reference value used for link selection in STP. STP calculates path costs to select the most robust links and block redundant links that are less robust, to prune the network into a loop-free tree.

NOTE:

All the ports on the root bridge are designated ports.

How STP works

The devices on a network exchange BPDUs to identify the network topology. Configuration BPDUs contain sufficient information for the network devices to complete spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID: Comprises the priority and MAC address of the root bridge.

- Root path cost: The cost of the path to the root bridge.
- Designated bridge ID: Comprises the priority and MAC address of the designated bridge.
- Designated port ID: Comprises the port priority and global port number.
- Message age: age of the configuration BPDU while it propagates in the network.
- Max age: The maximum age of the configuration BPDU.
- Hello time: The transmission interval of the configuration BPDU.
- Forward delay: The delay before a port transitions to the forwarding state.

NOTE:

For simplicity, the descriptions and examples in this document involve only the following fields in the configuration BPDUs:

- Root bridge ID (represented by device priority)
 - Root path cost
 - Designated bridge ID (represented by device priority)
 - Designated port ID (represented by port name)
-

Calculation process of the STP algorithm

- Initial state

Upon initialization of a device, each port generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.

- Selection of the optimum configuration BPDU

Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.

The process of selecting the optimum configuration BPDU is as follows:

1. Selection of the optimum configuration BPDU

Step	Actions
1	<p>Upon receiving a configuration BPDU on a port, the device performs the following:</p> <ul style="list-style-type: none"> • If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device discards the received configuration BPDU and does not process the configuration BPDU of this port. • If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device replaces the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.
2	The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.

NOTE:

The following are the principles of configuration BPDU comparison:

The configuration BPDU with the lowest root bridge ID has the highest priority.

If the configuration BPDUs have the same root bridge ID, their root path costs are compared. Assume that the root path cost in a configuration BPDU plus the path cost of a receiving port is S . The configuration BPDU with the smallest S value has the highest priority.

If all configuration BPDUs have the same ports value, their designated bridge IDs, designated port IDs, and the IDs of the receiving ports are compared in sequence. The configuration BPDU containing a smaller ID wins out.

- Selection of the root bridge

Initially, each STP-enabled device on the network assumes itself to be the root bridge, with the root bridge ID being its own device ID. By exchanging configuration BPDUs, the devices compare their root bridge IDs to elect the device with the smallest root bridge ID as the root bridge.

- Selection of the root port and designated ports on a non-root device

2. Selection of the root port and designated ports

Step	Description
1	A non-root device regards the port on which it received the optimum configuration BPDU as the root port.
2	Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of its other ports. <ul style="list-style-type: none">• The root bridge ID is replaced with that of the configuration BPDU of the root port.• The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost of the root port.• The designated bridge ID is replaced with the ID of this device.• The designated port ID is replaced with the ID of this port.
3	The device compares the calculated configuration BPDU with the configuration BPDU on the port whose port role is to be determined: <ul style="list-style-type: none">• If the calculated configuration BPDU is superior, the device considers this port as the designated port, replaces the configuration BPDU on the port with the calculated configuration BPDU, and periodically sends out the calculated configuration BPDU.• If the configuration BPDU on the port is superior, the device blocks this port without updating its configuration BPDU. The blocked port can receive BPDUs, but cannot send BPDUs or forward data.

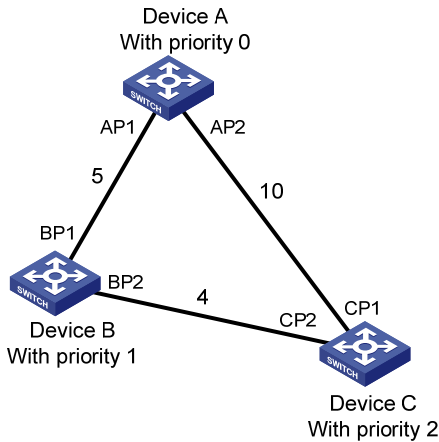
NOTE:

When the network topology is stable, only the root port and designated ports forward traffic, while other ports are all in the blocked state to receive BPDUs but not to forward BPDUs or user traffic.

A tree-shape topology forms when the root bridge, root ports, and designated ports are selected.

The following describes how the STP algorithm works.

a. Network diagram for the STP algorithm



As shown in a, the priority values of Device A, Device B, and Device C are 0, 1, and 2, and the path costs of links among the three devices are 5, 10 and 4 respectively.

- Initial state of each device

3. Initial state of each device

Device	Port name	BPDU of port
Device A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}
Device B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}
Device C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP2}

- Comparison process and result on each device

4. Comparison process and result on each device

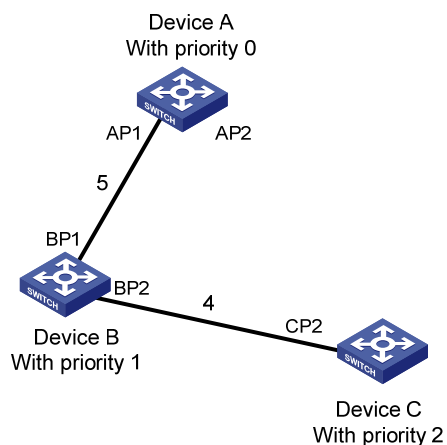
Device	Comparison process	Configuration BPDU on ports after comparison
Device A	<ul style="list-style-type: none"> • Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU. • Port AP2 receives the configuration BPDU of Device C {2, 0, 2, CP1}. Device A finds that the BPDU of the local port {0, 0, 0, AP2} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU. • Device A finds that both the root bridge and designated bridge in the configuration BPDUs of all its ports are itself, so it assumes itself to be the root bridge. In this case, it does not make any change to the configuration BPDU of each port, and starts sending out configuration BPDUs periodically. 	AP1: {0, 0, 0, AP1} AP2: {0, 0, 0, AP2}

Device	Comparison process	Configuration BPDU on ports after comparison
Device B	<ul style="list-style-type: none"> Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0, 1, BP1}, and updates the configuration BPDU of BP1. Port BP2 receives the configuration BPDU of Device C {2, 0, 2, CP2}. Device B finds that the configuration BPDU of the local port {1, 0, 1, BP2} is superior to the received configuration BPDU, and therefore discards the received configuration BPDU. 	BP1: {0, 0, 0, AP1} BP2: {1, 0, 1, BP2}
	<ul style="list-style-type: none"> Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed. Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}. Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically. 	Root port BP1: {0, 0, 0, AP1} Designated port BP2: {0, 5, 1, BP2}
Device C	<ul style="list-style-type: none"> Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and updates the configuration BPDU of CP1. Port CP2 receives the configuration BPDU of port BP2 of Device B {1, 0, 1, BP2} before the configuration BPDU is updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP2}, and therefore updates the configuration BPDU of CP2. 	CP1: {0, 0, 0, AP2} CP2: {1, 0, 1, BP2}
	After comparison: <ul style="list-style-type: none"> The configuration BPDU of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed. Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU. 	Root port CP1: {0, 0, 0, AP2} Designated port CP2: {0, 10, 2, CP2}
	<ul style="list-style-type: none"> Then, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its own configuration BPDU, Device C launches a BPDU update process. At the same time, port CP1 receives periodic configuration BPDUs from Device A. Device C does not launch an update process after comparison. 	CP1: {0, 0, 0, AP2} CP2: {0, 5, 1, BP2}

Device	Comparison process	Configuration BPDU on ports after comparison
	<p>After comparison:</p> <ul style="list-style-type: none"> Because the root path cost of CP2 (9) (root path cost of the BPDU (5) plus path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed. After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new event, for example, the link from Device B to Device C going down. 	<p>Blocked port CP2: {0, 0, 0, AP2}</p> <p>Root port CP2: {0, 5, 1, BP2}</p>

After the comparison processes described in 4, a spanning tree with Device A as the root bridge is established, and the topology is shown in a.

a. The final calculated spanning tree



NOTE:

This example shows a simplified spanning tree calculation process.

The configuration BPDU forwarding mechanism in STP

The configuration BPDUs of STP are forwarded following these guidelines:

- Upon network initiation, every device regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular hello interval.
- If it is the root port that received a configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device increases the message age carried in the configuration BPDU following a certain rule and starts a timer to time the configuration BPDU while sending out this configuration BPDU through the designated port.
- If the configuration BPDU received on a designated port has a lower priority than the configuration BPDU of the local port, the port immediately sends out its own configuration BPDU in response.

- If a path becomes faulty, the root port on this will no longer receives new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. The device generates a configuration BPDU with itself as the root and sends out the BPDUs and TCN BPDUs. This triggers a new spanning tree calculation process to establish a new path to restore the network connectivity.

However, the newly calculated configuration BPDU cannot be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data along the old path. If the new root ports and designated ports begin to forward data as soon as they are elected, a temporary loop may occur.

STP timers

STP calculation involves the following timers: forward delay, hello time, and max age.

- Forward delay

Forward delay is the delay time for state transition.

A path failure can cause spanning tree re-calculation to adapt the spanning tree structure to the change. However, the resulting new configuration BPDU cannot propagate throughout the network immediately. If the newly elected root ports and designated ports start to forward data right away, a temporary loop is likely to occur.

For this reason, as a mechanism for state transition in STP, the newly elected root ports or designated ports require twice the forward delay time before transitioning to the forwarding state to ensure that the new configuration BPDU has propagated throughout the network.

- Hello time

The device sends hello packets at the hello time interval to the neighboring devices to ensure that the paths are fault-free.

- Max age

The device uses the max age to determine whether a stored configuration BPDU has expired and discards it if the max age is exceeded.

RSTP

RSTP achieves rapid network convergence by allowing a newly elected root port or designated port to enter the forwarding state much faster under certain conditions than STP.

A newly elected RSTP root port rapidly enters the forwarding state if the old root port on the device has stopped forwarding data and the upstream designated port has started forwarding data.

A newly elected RSTP designated port rapidly enters the forwarding state if it is an edge port (which directly connects to a user terminal rather than to another network device or a shared LAN segment) or it connects to a point-to-point link (to another device). Edge ports directly enter the forwarding state. Connecting to a point-to-point link, a designated port enters the forwarding state immediately after the device receives a handshake response from the directly connected device.

MSTP

STP and RSTP limitations

STP does not support rapid state transition of ports. A newly elected port must wait twice the forward delay time before transitioning to the forwarding state, even if it connects to a point-to-point link or is an edge port.

Although RSTP supports rapid network convergence, it has the same drawback as STP—All bridges within a LAN share the same spanning tree, so redundant links cannot be blocked based on VLAN, and the packets of all VLANs are forwarded along the same spanning tree.

MSTP features

Developed based on IEEE 802.1s, MSTP overcomes the shortcomings of STP and RSTP. In addition to supporting for rapid network convergence, it also provides a better load sharing mechanism for redundant links by allowing data flows of different VLANs to be forwarded along separate paths.

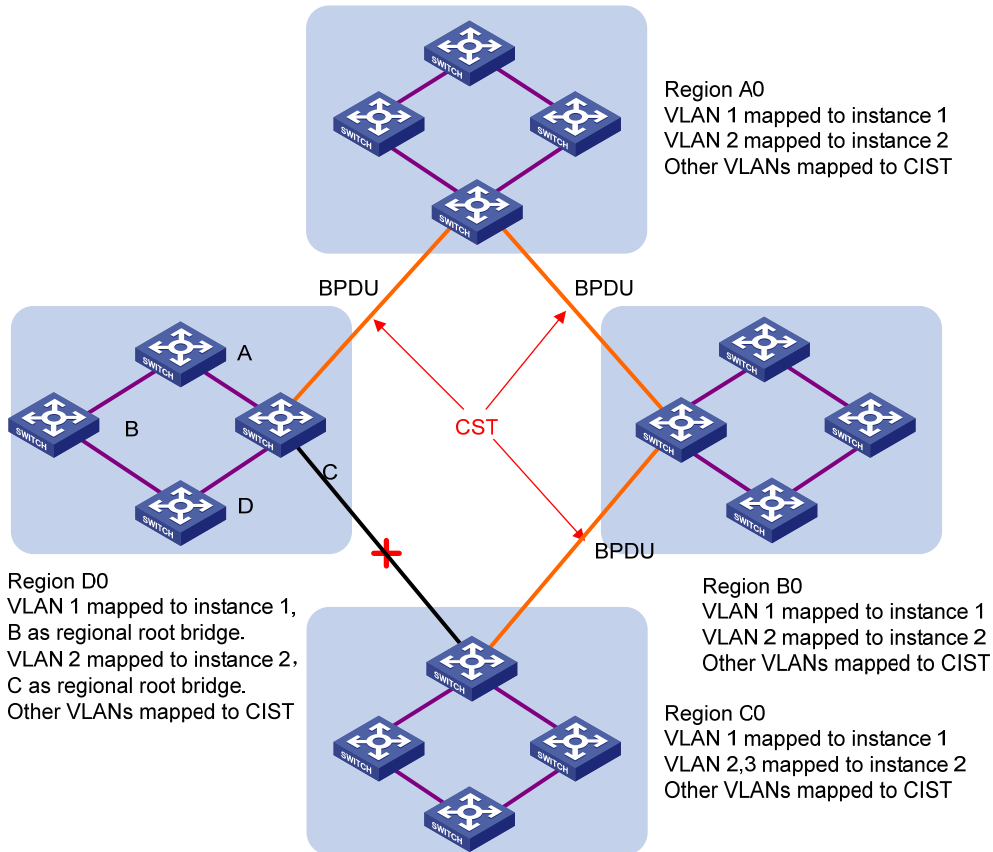
MSTP includes the following features:

- MSTP supports mapping VLANs to MST instances (MSTIs) by means of a VLAN-to-MSTI mapping table. MSTP can reduce communication overheads and resource usage by mapping multiple VLANs to one MSTI.
- MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.
- MSTP prunes a loop network into a loop-free tree, avoiding proliferation and endless cycling of packets in a loop network. In addition, it provides multiple redundant paths for data forwarding, supporting load balancing of VLAN data.
- MSTP is compatible with STP and RSTP.

MSTP basic concepts

Assume that all the four devices in [a](#) are running MSTP. This section explains some basic concepts of MSTP based on the figure.

a. Basic concepts in MSTP



MST region

A multiple spanning tree region (MST region) consists of multiple devices in a switched network and the network segments among them. All these devices have the following characteristics:

- MSTP-enabled
- Same region name
- Same VLAN-to-MSTI mapping configuration
- Same MSTP revision level
- Physically linked together

All the devices in region A0 in a have the same MST region configuration:

- The same region name
- The same VLAN-to-MSTI mapping configuration (VLAN 1 is mapped to MSTI 1, VLAN 2 to MSTI 2, and the rest to the common and internal spanning tree (CIST, that is, MSTI 0))
- The same MSTP revision level (not shown in the figure)

Multiple MST regions can exist in a switched network. You can assign multiple devices to the same MST region.

VLAN-to-MSTI mapping table

As an attribute of an MST region, the VLAN-to-MSTI mapping table describes the mapping relationships between VLANs and MSTIs. In a, the VLAN-to-MSTI mapping table of region A0 is: VLAN 1 is mapped to

MSTI 1, VLAN 2 to MSTI 2, and the rest to CIST. MSTP achieves load balancing by means of the VLAN-to-MSTI mapping table.

IST

An internal spanning tree (IST) is a spanning tree that runs in an MST region. It is also called MSTI 0, a special MSTI to which all VLANs are mapped by default.

In [a](#), the CIST has a section in each MST region, and this section is the IST in the respective MST region.

CST

The common spanning tree (CST) is a single spanning tree that connects all MST regions in a switched network. If you regard each MST region as a device, the CST is a spanning tree calculated by these devices through STP or RSTP.

The red lines in [a](#) represent the CST.

CIST

The common and internal spanning tree (CIST) is a single spanning tree that connects all devices in a switched network. It consists of the ISTs in all MST regions and the CST.

In [a](#), the ISTs (MSTI 0) in all MST regions plus the inter-region CST constitute the CIST of the entire network.

MSTI

Multiple spanning trees can be generated in an MST region through MSTP, one spanning tree being independent of another. Each spanning tree is referred to as a multiple spanning tree instance (MSTI).

In [a](#), for example, multiple MSTIs can exist in each MST region, each MSTI corresponding to the specified VLANs.

Regional root

The root bridge of the IST or an MSTI within an MST region is the regional root of the IST or MSTI. Based on the topology, different spanning trees in an MST region may have different regional roots.

In region D0 in [a](#), the regional root of MSTI 1 is device B, while that of MSTI 2 is device C.

Common root bridge

The common root bridge is the root bridge of the CIST.

In [a](#), the common root bridge is a device in region A0.

Boundary port

A boundary port is a port that connects an MST region to another MST region, or to a single spanning-tree region running STP, or to a single spanning-tree region running RSTP. It is at the boundary of an MST region.

During MSTP calculation, the role of a boundary port in an MSTI must be consistent with its role in the CIST. But this is not true with master ports. A master port on MSTIs is a root port on the CIST. For example, in [a](#), if a device in region A0 is interconnected with the first port of a device in region D0 and the common root bridge of the entire switched network is located in region A0, the first port of that device in region D0 is the boundary port of region D0.

Port roles

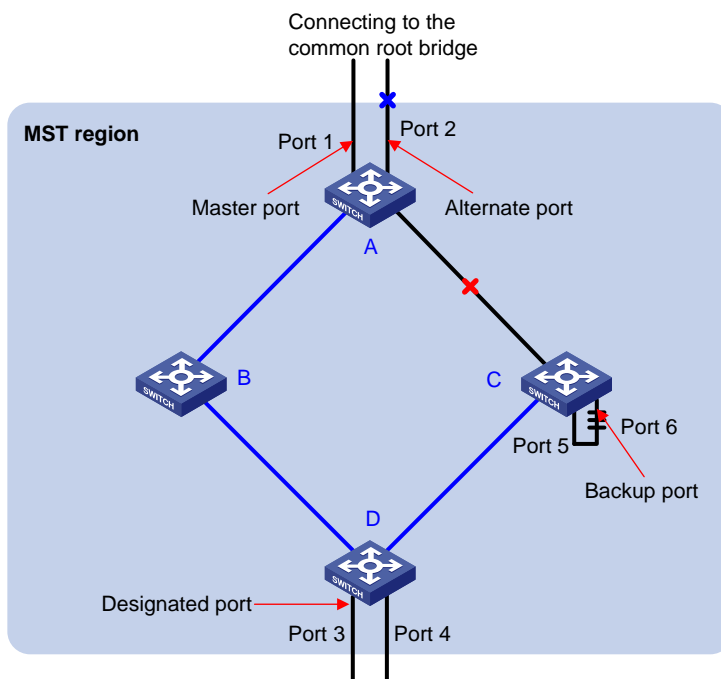
MSTP calculation involves the following port roles:

- Root port: Forwards data for a non-root bridge to the root bridge.

- Designated port: Forwards data to the downstream network segment or device.
- Master port: A port on the shortest path from the local MST region to the common root bridge, connecting the MST region to the common root bridge. If the region is seen as a node, the master port is the root port of the region on the CST. The master port is a root port on IST or CIST and still a master port on the other MSTIs.
- Alternate port: The backup port for a root port and master port. When the root port or master port is blocked, the alternate port takes over.
- Backup port: The backup port of a designated port. When the designated port is invalid, the backup port becomes a new designated port and starts forwarding data without delay. A loop occurs when two ports of the same MSTP device are interconnected, so the device blocks one of the ports. The blocked port acts as the backup.

A port can play different roles in different MSTIs.

a. Port roles



In a, devices A, B, C, and D constitute an MST region. Port 1 and port 2 of device A are connected to the common root bridge, port 5 and port 6 of device C form a loop, port 3 and port 4 of Device D are connected downstream to the other MST regions.

Port states

In MSTP, a port may be in one of the following states:

- Forwarding: The port learns MAC addresses and forwards user traffic.
- Learning: The port learns MAC addresses but does not forward user traffic.
- Discarding: The port does not learn MAC addresses or forwards user traffic.

NOTE:

When in different MSTIs, a port can be in different states.

A port state is not exclusively associated with a port role. 1 lists the port states supported by each port role, where “√” indicates that the port supports the state and “—” indicates that the port does not support the state.

1. Ports states supported by different port roles

Port role (right)	Root port/master port	Designated port	Boundary port	Alternate port	Backup port
Forwarding	√	√	√	—	—
Learning	√	√	√	—	—
Discarding	√	√	√	√	√

How MSTP works

MSTP divides an entire Layer 2 network into multiple MST regions, which are interconnected by a calculated CST. Inside an MST region, multiple spanning trees, called MSITs, are calculated. Among these MSITs, MSTI 0 is the CIST.

Similar to STP, MSTP uses configuration BPDUs to calculate spanning trees. However, an important difference is that an MSTP BPDU carries the MSTP configuration on the device from which this BPDU is sent.

CIST calculation

The calculation of a CIST tree is also the process of configuration BPDU comparison. During this process, the device with the highest priority is elected as the root bridge of the CIST. MSTP generates an IST within each MST region through calculation, and, at the same time, MSTP regards each MST region as a single device and generates a CST among these MST regions through calculation. The CST and ISTs constitute the CIST of the entire network.

MSTI calculation

Within an MST region, MSTP generates different MSTIs for different VLANs based on the VLAN-to-MSTI mappings. For each spanning tree, MSTP performs a separate calculation process similar to spanning tree calculation in STP. For more information, see “How STP works”.

In MSTP, a VLAN packet is forwarded along the following paths:

- Within an MST region, the packet is forwarded along the corresponding MSTI.
- Between two MST regions, the packet is forwarded along the CST.

Implementation of MSTP on devices

MSTP is compatible with STP and RSTP. STP and RSTP protocol packets can be recognized by devices running MSTP and used for spanning tree calculation.

In addition to basic MSTP functions, the following functions are provided for ease of management:

- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard

- Loop guard
- TC-BPDU (a message that notifies the device of topology changes) guard

Protocols and standards

- IEEE 802.1d, *Media Access Control (MAC) Bridges*
- IEEE 802.1w, *Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration*
- IEEE 802.1s, *Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees*

Configuring MSTP

Configuration task list

Perform the tasks described in 1 to configure MSTP.

1. MSTP configuration task list

Task	Remarks
Configuring an MST region	Optional Configure the MST region-related parameters and VLAN-to-MSTI mappings. By default, the MST region-related parameters adopt the default values, and all VLANs in an MST region are mapped to MSTI 0.
Configuring MSTP globally	Required Enable MSTP globally and configure MSTP parameters. By default, MSTP is enabled globally; and all MSTP parameters have default values.
Configuring MSTP on a port	Optional Enable MSTP on a port and configure MSTP parameters. By default, MSTP is enabled on a port, and all MSTP parameters adopt the default values.
Displaying MSTP information of a port	Optional Display MSTP information of a port in MSTI 0, the MSTI to which the port belongs, and the path cost and priority of the port.

Configuring an MST region

Select **Network** → **MSTP** from the navigation tree to enter the page as shown in [a](#).

a. MST region

Region	Global	Port Summary	Port Setup
Format Selector		Region Name	Revision Level
0		00e0fc003620	0

[Modify](#)

Instance	VLAN Mapped
0	1 to 4094

Click **Modify** to enter the page shown in b.

b. Configure an MST region

Region	Global	Port Summary	Port Setup
--------	--------	--------------	------------

Region Name (1-32 Chars.)

Revision Level (0-65535, Default = 0)

Manual Modulo

Instance ID (Example: 1,3,5-10)

[Apply](#) [Remove](#)

Instance ID	VLAN Mapped

[Activate](#) [Cancel](#)

2. Configuration items of configuring an MST region

Item	Description				
Region Name	MST region name. The MST region name is the bridge MAC address of the device by default.				
Revision Level	Revision level of the MST region.				
Manual	<table border="1"> <thead> <tr> <th>Instance ID</th> <th>VLAN ID</th> </tr> </thead> <tbody> <tr> <td colspan="2">Manually add VLAN-to-MSTI mappings. Click Apply to add the VLAN-to-MSTI mapping entries to the list below.</td> </tr> </tbody> </table>	Instance ID	VLAN ID	Manually add VLAN-to-MSTI mappings. Click Apply to add the VLAN-to-MSTI mapping entries to the list below.	
Instance ID	VLAN ID				
Manually add VLAN-to-MSTI mappings. Click Apply to add the VLAN-to-MSTI mapping entries to the list below.					
Modulo	Modulo Value The device automatically maps 4094 VLANs to the corresponding MSTIs based on the modulo value.				

Return to [MSTP configuration task list](#).

Configuring MSTP globally

Select **Network** → **MSTP** from the navigation tree, and click the **Global** tab to enter the page shown in a.

a. Configure MSTP globally

Region	Global	Port Summary	Port Setup
Global MSTP Configuration			
Enable STP Globally:	Enable		
BPDU Protection:	Disable		
Mode:	MSTP		
Max Hops:	20		
Path Cost Standard:	Legacy		
<input type="checkbox"/> Bridge Diameter:	7		
<input type="checkbox"/> Timer(in centiseconds)			
Forward Delay:	1500	(400-3000, Must be a multiple of 100)	
Hello Time:	200	(100-1000, Must be a multiple of 100)	
Max Age:	2000	(600-4000, Must be a multiple of 100)	
<input type="checkbox"/> Instance:			
Instance ID:	0		
Root Type:	Not Set		
Bridge Priority:	32768		
TC Protection:	Enable		
TC Protection Threshold:	6	(1-255, default=6)	
Apply			

2. Configuration items of MSTP global configuration

Item	Description
Enable STP Globally	Globally enable or disable STP. Other MSTP configurations take effect only after you globally enable STP.
BPDU Protection	Enable or disable BPDU guard. BPDU guard can protect the device from malicious BPDU attacks, making the network topology stable.

Item	Description	
Mode	<p>Set the STP working mode:</p> <ul style="list-style-type: none"> • STP—Each port on a device sends out STP BPDUs. • RSTP—Each port on a device sends out RSTP BPDUs, and automatically migrates to STP-compatible mode when detecting that it is connected with a device running STP. • MSTP—Each port on a device sends out MSTP BPDUs, and automatically migrates to STP-compatible mode when detecting that it is connected with a device running STP. <p>The working mode is RSTP by default.</p>	
Max Hops	<p>Set the maximum number of hops in an MST region to restrict the region size. The setting can take effect only when it is configured on the regional root bridge.</p>	
Path Cost Standard	<p>Specify the standard for path cost calculation. Options include Legacy, IEEE 802.1D-1998, and IEEE 802.1T.</p>	
Bridge Diameter	<p>Any two stations in a switched network are interconnected through a specific path composed of a series of devices. The bridge diameter (or the network diameter) is the number of devices on the path composed of the most devices.</p> <p>After you set the network diameter, you cannot set the timers. Instead, the device automatically calculates the forward delay, hello time, and max age.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> • The configured network diameter is effective only for the CIST, not for MSTIs. • The bridge diameter cannot be configured together with the timers. 	
Timer	<p>Forward Delay</p> <p>Set the delay for the root and designated ports to transit to the forwarding state.</p>	<p>! IMPORTANT:</p> <ul style="list-style-type: none"> • The settings of hello time, forward delay, and max age must meet a certain formula. Otherwise, the network topology will not be stable. HP recommends you set the network diameter and then have the device automatically calculate the timers. • The bridge diameter cannot be configured together with the timers.
	<p>Hello Time</p> <p>Set the interval at which the device sends hello packets to the surrounding devices to ensure that the paths are fault-free.</p>	
	<p>Max Age</p> <p>Set the maximum length of time a configuration BPDU can be held by the device.</p>	
Instance	<p>Instance ID</p> <p>Set the role of the device in the MSTI or the bridge priority of the device, which is one of the factors determining whether the device can be elected as the root bridge.</p> <p>Roles of the device in the MSTI include:</p>	
	<p>Root Type</p> <ul style="list-style-type: none"> • Not Set—The device role is not set. You can set the bridge priority of the device when selecting this role. • Primary—Configure the device as the root bridge. You cannot set the bridge priority of the device when selecting this role. 	
	<p>Bridge Priority</p> <ul style="list-style-type: none"> • Secondary—Configure the device as a secondary root bridge. You cannot set the bridge priority of the device when selecting this role. 	

Item	Description
TC Protection	<p>Enable or disable TC-BPDU guard.</p> <p>When receiving topology change (TC) BPDUs, the device flushes its forwarding address entries. If someone forges TC-BPDUs to attack the device, the device will receive a large number of TC-BPDUs within a short time and frequently flushes its forwarding address entries. This affects network stability.</p> <p>With the TC-BPDU guard function, you can prevent frequent flushing of forwarding address entries.</p> <p>! IMPORTANT:</p> <p>HP does not recommend you to disable this function.</p>
TC Protection Threshold	Set the maximum number of immediate forwarding address entry flushes the device can perform within a certain period of time after receiving the first TC-BPDU.

Return to [MSTP configuration task list](#).

Configuring MSTP on a port

Select **Network** → **MSTP** from the navigation tree, and click the **Port Setup** tab to enter the page shown in a.

a. MSTP configuration on a port

2. Configuration items of configuring MSTP on a port

Item	Description
STP	Enable or disable STP on the port.

Item	Description	
Protection	<p>Set the type of protection to be enabled on the port:</p> <ul style="list-style-type: none"> • Not Set—No protection is enabled on the port. • Edged Port, Root Protection, Loop Protection—For more information, see 3. 	
Instance	<p>Instance ID</p> <p>Port Priority</p> <p>Auto Path Cost</p>	<p>Set the priority and path cost of the port in the current MSTI.</p> <ul style="list-style-type: none"> • The priority of a port is an important factor in determining whether or not the port can be elected as the root port of a device. If all other conditions are the same, the port with the highest priority will be elected as the root port. On an MSTP-enabled device, a port can have different priorities in different MSTIs, and the same port can play different roles in different MSTIs, so that data of different VLANs can be propagated along different physical paths, thus implementing per-VLAN load balancing. You can set port priority values based on the actual networking requirements.
	Manual Path Cost	<ul style="list-style-type: none"> • Path cost is a parameter related to the rate of a port. On an MSTP-enabled device, a port can have different path costs in different MSTIs. Setting appropriate path costs allows VLAN traffic flows to be forwarded along different physical links, thus achieving VLAN-based load balancing. The device can automatically calculate the default path cost; alternatively, you can also manually configure path cost for ports.
	Point to Point	<p>Specify whether or not the port is connected to a point-to-point link:</p> <ul style="list-style-type: none"> • Auto—The link type of the port is automatically detected. • Force False—The link type for the port is not point-to-point link. • Force True—The link type for the port is point-to-point link. <p>ⓘ IMPORTANT:</p> <p>If a port is configured as connecting to a point-to-point link, the setting takes effect for the port in all MSTIs. If the physical link to which the port connects is not a point-to-point link but you force it to be a point-to-point link by configuration, the configuration may cause a temporary loop.</p>
	Advanced	<p>Transmit Limit</p>
	MSTP Mode	<p>Set whether or not the port migrates to the MSTP mode.</p> <p>In a switched network, if a port on an MSTP (or RSTP) device connects to a device running STP, this port will automatically migrate to the STP-compatible mode. After the device running STP is removed, the port on the MSTP (or RSTP) device may not be able to migrate automatically to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode. You can set this option to enable the port to automatically migrate to the MSTP (or RSTP) mode.</p>
Select port(s)	<p>Select one or multiple ports on which you want to configure MSTP on the chassis front panel. If aggregate interfaces are configured on the device, the page displays a list of aggregate interfaces below the chassis front panel. You can select aggregate interfaces from this list.</p>	

3. Protection types

Protection type	Description
Edged Port	<p>Set the port as an edge port.</p> <p>Some ports of access layer devices are directly connected to PCs or file servers, which cannot generate BPDUs. You can set these ports as edge ports to achieve fast transition for these ports.</p> <p>HP recommends you to enable the BPDU guard function in conjunction with the edged port function to avoid network topology changes when the edge ports receive configuration BPDUs.</p>
Root Protection	<p>Enable the root guard function.</p> <p>Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes a new root bridge to be elected and network topology change to occur. The root guard function is used to address such a problem.</p>
Loop Protection	<p>Enable the loop guard function.</p> <p>By keeping receiving BPDUs from the upstream device, a device can maintain the state of the root port and other blocked ports. These BPDUs may get lost because of network congestion or unidirectional link failures. In this case, the device will re-elect a root port, and blocked ports may transit to the forwarding state, causing loops in the network. The loop guard function is used to address such a problem.</p>

Return to [MSTP configuration task list](#).

Displaying MSTP information of a port

Select **Network** → **MSTP** from the navigation tree, and click the **Port Summary** tab to enter the page shown in [a](#).

a. The Port Summary tab

Select a port

HP V1910-16G Sw...

Instance 0

```

----[Port16(GigabitEthernet1/0/16)] [FORWARDING]----
Port Protocol      :enabled
Port Role          :CIST Designated Port
Port Priority       :128
Port Cost(Legacy)  :Config=auto / Active=20
Desg. Bridge/Port  :32768.000f-e000-0002 / 128.16
Port Edged         :Config=enabled / Active=disabled
  
```

Instance	Cost	Priority
----------	------	----------

Select a port (GigabitEthernet 1/0/16 for example) on the chassis front panel. If aggregate interfaces are configured on the device, the page displays a list of aggregate interfaces below the chassis front panel, and you can select aggregate interfaces from this list. The lower part of the page displays the MSTP information of the port in MSTI 0 (when STP is enabled globally) or the STP status and statistics (when STP is disabled globally), the MSTI to which the port belongs, and the path cost and priority of the port in the MSTI.

2. Fields in the displayed MSTP information of GigabitEthernet 1/0/16 in MSTI 0

Field	Description
[FORWARDING]	The port is in forwarding state. The port learns MAC addresses and forwards user traffic.
[LEARNING]	The port is in learning state. The port learns MAC addresses but does not forward user traffic.
[DISCARDING]	The port is in discarding state. The port does not learn MAC addresses or forward user traffic.
[DOWN]	The port is down.
Port Protocol	Whether or not STP is enabled on the port.
Port Role	The role of the port, which can be Alternate , Backup , Root , Designated , Master , or Disabled .
Port Priority	The priority of the port.

Field	Description
Port Cost(Legacy)	Path cost of the port. The field in the bracket indicates the standard used for port path cost calculation, which can be Legacy , dot1d-1998 , or dot1t . <ul style="list-style-type: none"> • Config indicates the configured value. • Active indicates the actual value.
Desg. Bridge/Port	Designated bridge ID and port ID of the port. The port ID displayed is insignificant for a port that does not support port priority.
Port Edged	Whether or not the port is an edge port: <ul style="list-style-type: none"> • Config indicates the configured value. • Active indicates the actual value.
Point-to-point	Whether or not the port is connected to a point-to-point link: <ul style="list-style-type: none"> • Config indicates the configured value. • Active indicates the actual value.
Transmit Limit	The maximum number of packets sent within each hello time.
Protection Type	Protection type on the port: <ul style="list-style-type: none"> • Root—Root guard • Loop—Loop guard • BPDU—BPDU guard • None—No protection
MST BPDU Format	Format of the MST BPDUs that the port can send, which can be legacy or 802.1s . <ul style="list-style-type: none"> • Config indicates the configured value. • Active indicates the actual value.
Port Config-Digest-Snooping	Whether or not digest snooping is enabled on the port.
Rapid transition	Whether or not the current port rapidly transitions to the forwarding state.
Num of Vlans Mapped	Number of VLANs mapped to the current MSTI.
PortTimes	Major parameters for the port: <ul style="list-style-type: none"> • Hello—Hello timer • MaxAge—Max Age timer • FWDly—Forward delay timer • MsgAge—Message Age timer • Remain Hop—Remaining hops
BPDU Sent	Statistics on sent BPDUs.
BPDU Received	Statistics on received BPDUs.
Protocol Status	Whether or not MSTP is enabled.
Protocol Std.	MSTP standard.
Version	MSTP version.
CIST Bridge-Prio.	Priority of the current device in the CIST.
MAC address	MAC address of the current device.

Field	Description
Max age(s)	Maximum age of a configuration BPDU.
Forward delay(s)	Port state transition delay, in seconds.
Hello time(s)	Configuration BPDU transmission interval, in seconds.
Max hops	Maximum hops of the current MST region.

Return to [MSTP configuration task list](#).

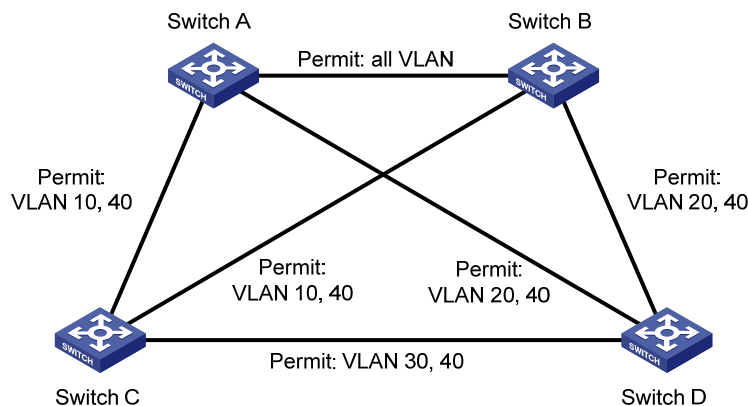
MSTP configuration example

Network requirements

Configure MSTP in the network shown in [a](#) to enable packets of different VLANs to be forwarded along different MSTIs.

- All devices on the network are in the same MST region.
- Packets of VLAN 10, VLAN 20, VLAN 30, and VLAN 40 are forwarded along MSTI 1, MSTI 2, MSTI 3, and MSTI 0 respectively.
- Switch A and Switch B operate at the distribution layer; Switch C and Switch D operate at the access layer. VLAN 10 and VLAN 20 are terminated on the distribution layer devices, and VLAN 30 is terminated on the access layer devices, so the root bridges of MSTI 1 and MSTI 2 are Switch A and Switch B respectively, while the root bridge of MSTI 3 is Switch C.

a. Network diagram for MSTP configuration



NOTE:

“Permit” next to a link in the figure is followed by the VLANs the packets of which are permitted to pass this link.

Configuration procedure

Table 48 Configure Switch A.

Configure an MST region.

- Select **Network** → **MSTP** from the navigation tree to enter the page shown in [b](#).

b. The Region tab

Region	Global	Port Summary	Port Setup
Format Selector	Region Name	Revision Level	
0	00e0fc003620	0	
<input type="button" value="Modify"/>			
Instance	VLAN Mapped		
0	1 to 4094		

- Click **Modify** to enter the page shown in c.

c. Configure an MST region

Region	Global	Port Summary	Port Setup
Region Name	<input type="text" value="example"/> (1-32 Chars.)		
Revision Level	<input type="text" value="0"/> (0-65535, Default = 0)		
<input checked="" type="radio"/> Manual <input type="radio"/> Modulo			
Instance ID	<input type="text" value="3"/>	VLAN ID	<input type="text"/> (Example:1,3,5-10)
			<input type="button" value="Apply"/> <input type="button" value="Remove"/>
Instance ID	VLAN Mapped		
1	10		
2	20		
3	30		
<input type="button" value="Activate"/> <input type="button" value="Cancel"/>			

- Type the region name **example**.
- Set the revision level to 0.
- Select the **Manual** option.
- Select **1** in the **Instance ID** drop-down list.
- Type the VLAN ID 10.
- Click **Apply** to map VLAN 10 to MSTI 1 and add the VLAN-to-MSTI mapping entry to the VLAN-to-MSTI mapping list.
- Repeat the previous steps to map VLAN 20 to MSTI 2 and VLAN 30 to MSTI 3, and add the VLAN-to-MSTI mapping entries to the VLAN-to-MSTI mapping list.
- Click **Activate**.

Configure MSTP globally.

- Select **Network** → **MSTP** from the navigation tree, and click the **Global** tab to enter the page shown in d.

d. **Configure MSTP globally (on Switch A)**

Region	Global	Port Summary	Port Setup
--------	--------	--------------	------------

Global MSTP Configuration

Enable STP Globally:	Enable	▼
BPDU Protection:	Disable	▼
Mode:	MSTP	▼
Max Hops:	20	▼
Path Cost Standard:	Legacy	▼

<input type="checkbox"/> Bridge Diameter:	7	▼
<input type="checkbox"/> Timer(in centiseconds)		
Forward Delay:	1500	(400-3000, Must be a multiple of 100)
Hello Time:	200	(100-1000, Must be a multiple of 100)
Max Age:	2000	(600-4000, Must be a multiple of 100)

<input checked="" type="checkbox"/> Instance:		
Instance ID:	1	▼
Root Type:	Primary	▼
Bridge Priority:	32768	▼
TC Protection:	Enable	▼
TC Protection Threshold:	6	(1-255, default=6)

- Select **Enable** in the **Enable STP Globally** drop-down list.
- Select **MSTP** in the **Mode** drop-down list.
- Select the **Instance** option.
- Type the Instance ID 1.
- Select **Primary** in the **Root Type** drop-down list.
- Click **Apply**.

Table 49 Configure Switch B.

Configure an MST region. The procedure is the same as that of configuring an MST region on Switch A.

Configure MSTP globally.

- Select **Network** → **MSTP** from the navigation tree, and click the **Global** tab to enter the page for configuring MSTP globally. See [d](#).
- Select **Enable** in the **Enable STP Globally** drop-down list.
- Select **MSTP** in the **Mode** drop-down list.
- Select the **Instance** option.
- Select **2** in the **Instance ID** drop-down list.
- Select **Primary** in the **Root Type** drop-down list.
- Click **Apply**.

Table 50 Configure Switch C.

Configure an MST region. The procedure is the same as that of configuring an MST region on Switch A.

Configure MSTP globally.

- Select **Network** → **MSTP** from the navigation tree, and click the **Global** tab to enter the page shown in [d](#).
- Select **Enable** in the **Enable STP Globally** drop-down list.
- Select **MSTP** in the **Mode** drop-down list.
- Select the **Instance** option.
- Select **3** in the **Instance ID** drop-down list.
- Select **Primary** in the **Root Type** drop-down list.
- Click **Apply**.

Table 51 Configure Switch D.

Configure an MST region. The procedure is the same as that of configuring an MST region on Switch A.

Configure MSTP globally.

- Select **Network** → **MSTP** from the navigation tree, and click the **Global** tab to enter the page shown in [e](#).

e. **Configure MSTP globally (on Switch D)**

Region	Global	Port Summary	Port Setup
--------	--------	--------------	------------

Global MSTP Configuration

Enable STP Globally:	Enable	▼
BPDU Protection:	Disable	▼
Mode:	MSTP	▼
Max Hops:	20	▼
Path Cost Standard:	Legacy	▼

<input type="checkbox"/> Bridge Diameter:	7	▼
<input type="checkbox"/> Timer(in centiseconds)		
Forward Delay:	1500	(400-3000, Must be a multiple of 100)
Hello Time:	200	(100-1000, Must be a multiple of 100)
Max Age:	2000	(600-4000, Must be a multiple of 100)

<input type="checkbox"/> Instance:		
Instance ID:	0	▼
Root Type:	Not Set	▼
Bridge Priority:	32768	▼
TC Protection:	Enable	▼
TC Protection Threshold:	6	(1-255, default=6)

- Select **Enable** in the **Enable STP Globally** drop-down list.
- Select **MSTP** in the **Mode** drop-down list.
- Click **Apply**.

Configuration guidelines

When configuring MSTP, follow these guidelines:

- Two devices belong to the same MST region only if they are interconnected through physical links, and share the same region name, the same MSTP revision level, and the same VLAN-to-MSTI mappings.
- If two or more devices have been designated to be root bridges of the same spanning tree instance, MSTP will select the device with the lowest MAC address as the root bridge.

- If the device is not enabled with BPDU guard, when a boundary port receives a BPDU from another port, it converts into a non-boundary port. To restore its port role as a boundary port, you need to restart the port.
- Configure ports that are directly connected to terminals as boundary ports and enable BPDU guard for them. These ports can rapidly transit to the forwarding state, and the network security can be ensured.

Link aggregation and LACP configuration

Ethernet link aggregation, or simply link aggregation, combines multiple physical Ethernet ports into one logical link, called an aggregate link. Link aggregation delivers the following benefits:

- Increases bandwidth beyond the limits of any single link. In an aggregate link, traffic is distributed across the member ports.
- Improves link reliability. The member ports dynamically back up one another. When a member port fails, its traffic is automatically switched to other member ports.

Basic concepts

Aggregate interface

An aggregate interface is a logical Layer 2 or Layer 3 aggregate interface.

NOTE:

The device supports Layer 2 aggregation interfaces only.

Aggregation group

An aggregation group is a group of Ethernet interfaces combined together. When you create an aggregate interface, the device automatically creates an aggregation group of the same type and number as the aggregate interface. For example, when you create interface Bridge-Aggregation 1, Layer 2 aggregation group 1 is created.

You can assign Layer 2 Ethernet interfaces only to a Layer 2 aggregation group, and Layer 3 Ethernet interfaces only to a Layer 3 aggregation group.

NOTE:

The device supports Layer 2 aggregation groups only.

Aggregation states of member ports in an aggregation group

A member port in an aggregation group can be in either of the following aggregation states:

- Selected: A Selected port can forward user traffic.
- Unselected: An Unselected port cannot forward user traffic.

The rate of an aggregate interface is the sum of the selected member ports' rates. The duplex mode of an aggregate interface is consistent with that of the selected member ports. All selected member ports use the same duplex mode.

For how the state of a member port is determined, see "[Static aggregation mode](#)" and "[Dynamic aggregation mode](#)".

LACP

The IEEE 802.3ad Link Aggregation Control Protocol (LACP) enables dynamic aggregation of physical links. It uses link aggregation control protocol data units (LACPDU) for exchanging aggregation information between LACP-enabled devices.

LACP is automatically enabled on interfaces in a dynamic aggregation group. For information about dynamic aggregation groups, see “[Dynamic aggregation mode](#)”. An LACP-enabled interface sends LACPDU to notify the remote system (the partner) of its system LACP priority, system MAC address, LACP port priority, port number, and operational key. Upon receiving an LACPDU, the partner compares the received information with the information received on other interfaces to determine the interfaces that can operate as selected interfaces. This allows the two systems to reach an agreement on which link aggregation member ports should be placed in Selected state.

Operational key

When aggregating ports, link aggregation control automatically assigns each port an operational key based on port attributes, including the port rate, duplex mode and link state configuration.

In an aggregation group, all selected ports are assigned the same operational key.

Class-two configurations

The contents of class-two configurations are listed in 1. A member port can be placed in the Selected state only if it has the same class-two configurations as the aggregate interface.

1. Class-two configurations

Type	Considerations
Port isolation	Whether a port has joined an isolation group.
VLAN	Permitted VLAN IDs, PVID, link type (trunk, hybrid, or access), and tag mode.
MAC address learning	MAC address learning limit.

NOTE:

Some configurations are called class-one configurations. Such configurations, for example, MSTP, can be configured on aggregate interfaces and member ports but are not considered during operational key calculation. For more information about MSTP configuration on member ports of link aggregation groups or aggregate interfaces, see the chapter “[MSTP configuration](#)”.

Any class-two configuration change may affect the aggregation state of link aggregation member ports and ongoing traffic. To make sure that you are aware of the risk, the system displays a warning message every time you attempt to change a class-two configuration setting on a member port. For more information about the port isolation configuration, VLAN configuration, and MAC address learning limit configuration on member ports of link aggregation groups or aggregate interfaces, see the chapters “[Port isolation configuration](#)”, “[VLAN configuration](#)”, and “[Port management configuration](#)”.

Link aggregation modes

Link aggregation has the following modes: dynamic and static.

Static aggregation mode

LACP is disabled on the member ports in a static aggregation group. In a static aggregation group, the system sets a port to Selected or Unselected state by the following rules:

- Select a port as the reference port from the ports that are in up state and have the same class-two configurations as the corresponding aggregate interface. The candidate ports are sorted by

aggregation priority, duplex, and speed in the following order (with the one at the top selected as the reference port):

- Lowest aggregation priority value
- Full duplex/high speed
- Full duplex/low speed
- Half duplex/high speed
- Half duplex/low speed
- Consider the ports in up state with the same port attributes and class-two configurations as the reference port as candidate Selected ports, and set all others in the Unselected state.
- Static aggregation limits the number of Selected ports in an aggregation group. When the number of the candidate Selected ports is under the limit, all the candidate Selected ports become Selected ports. When the limit is exceeded, set the candidate Selected ports with smaller port numbers in the Selected state and those with greater port numbers in the Unselected state.
- If all the member ports are down, set their states to Unselected.
- Set the ports that cannot aggregate with the reference port to the Unselected state.

NOTE:

If a static aggregation group has reached the limit on Selected ports, any port that joins the group is placed in the Unselected state to avoid traffic interruption on the current Selected ports. Avoid this situation, however, because it may cause the aggregation state of a port to change after a reboot.

Dynamic aggregation mode

LACP is automatically enabled on all member ports in a dynamic aggregation group.

In a dynamic aggregation group, the following rules apply:

- A Selected port can receive and transmit LACPDUs.
- An Unselected port can receive and send LACPDUs only if it is up and with the same configurations as those on the aggregate interface.

In a dynamic aggregation group, the system sets the ports to Selected or Unselected state using the following workflow:

Table 52 The local system (the actor) negotiates with the remote system (the partner) to determine port state based on the port IDs on the end with the preferred system ID. The following is the detailed negotiation procedure:

- Compare the system ID (comprising the system LACP priority and the system MAC address) of the actor with that of the partner. The system with the lower LACP priority wins out. If they are the same, compare the system MAC addresses. The system with the smaller MAC address wins out.
- Compare the port IDs of the ports on the system with the smaller system ID. A port ID comprises a port LACP priority and a port number. First compare the port LACP priorities. The port with the lower LACP priority wins out. If two ports are with the same LACP priority, compare their port numbers. The port with the smaller port ID, that is, the port with smaller port number, is selected as the reference port.
- If a port (in an up state) is with the same port attributes and class-two configuration as the reference port, and the peer port of the port is with the same port attributes and class-two configurations as the peer port of the reference port, consider the port as a candidate selected port; otherwise set the port to the Unselected state.

- The number of selected ports that an aggregation group can contain is limited. When the number of candidate selected ports is under the limit, all the candidate selected ports are set to Selected state. When the limit is exceeded, the system selects the candidate selected ports with smaller port IDs as the selected ports, and set other candidate selected ports to Unselected state. At the same time, the peer device, being aware of the changes, changes the state of its ports accordingly.

Table 53 Set the ports that cannot aggregate with the reference port to the Unselected state.

NOTE:

For static and dynamic aggregation modes:

In an aggregation group, the port to be a selected port must be the same as the reference port in port attributes, and class-two configurations. To keep these configurations consistent, you should manually configure the port.

Change a port attribute or class-two configuration setting for a port with caution, because the change may affect the aggregation state of member ports and interrupt services.

Load sharing mode of an aggregation group

Every link aggregation group created on HP V1910 Switch Series operates in load sharing mode all the time, even when it contains only one member port.

Configuring link aggregation and LACP

Configuration task list

Configuring a static aggregation group

Perform the tasks in 1 to configure a static aggregation group.

1. Static aggregation group configuration task list

Task	Remarks
Creating a link aggregation group	Required Create a static aggregate interface and configure member ports for the static aggregation group automatically created by the system when you create the aggregate interface. By default, no link aggregation group exists.
Displaying information of an aggregate interface	Optional Perform this task to view detailed information of an existing aggregation group.

Configuring a dynamic aggregation group

Perform the tasks in 1 to configure a dynamic aggregation group.

1. Dynamic aggregation group configuration task list

Task	Remarks
Creating a link aggregation group	Required Create a dynamic aggregate interface and configure member ports for the dynamic aggregation group automatically created by the system when you create the aggregate interface. LACP is enabled automatically on all the member ports. By default, no link aggregation group exists.
Displaying information of an aggregate interface	Optional Perform this task to view detailed information of an existing aggregation group.
Setting LACP priority	Optional Perform the task to set LACP priority for the local system and link aggregation member ports. Changes of LACP priorities affect the Selected/Unselected state of link aggregation member ports. The default port LACP priority and system LACP priority are both 32768.
Displaying information of LACP-enabled ports	Optional Perform the task to view detailed information of LACP-enabled ports and the corresponding remote (partner) ports.

Creating a link aggregation group

Select **Network** → **Link Aggregation** from the navigation tree, and click the **Create** tab to enter the page as shown in [a](#).

a. Create a link aggregation group

Summary	Create	Modify	Remove
---------	--------	--------	--------

Enter Link Aggregation Interface ID: (1-10)

Specify Interface Type: Static (LACP Disabled) Dynamic (LACP Enabled)

Note: The type of the link aggregation interface set here overwrites the existing LACP settings of the ports in the link aggregation interface.

Select port(s) for the link aggregation interface:

HP V1910-16G Sw...

Select All Select None

Selected Ports: ■ Members of the link aggregation interface to be created.

Unselected Ports:

- Not a member of any link aggregation interface, and LACP is disabled on this port.
- LACP has been enabled on this port.
- Members of existing link aggregation interfaces.

Summary:

Aggregation Interface ID	Member Ports	Aggregation Interface Type
1		Static

Apply Cancel

2. Configuration items of creating a link aggregation group

Item	Description
Enter Link Aggregation Interface ID	Assign an ID to the link aggregation group to be created. You can view the result in the Summary list box at the bottom of the page.
Specify Interface Type	Set the type of the link aggregation interface to be created: <ul style="list-style-type: none"> • Static (LACP Disabled) • Dynamic (LACP Enabled)
Select port(s) for the link aggregation interface	Select one or multiple ports to be assigned to the link aggregation group from the chassis front panel. You can view the result in the Summary list box at the bottom of the page.

Return to [Static aggregation group configuration task list](#).

Return to [Dynamic aggregation group configuration task list](#).

Displaying information of an aggregate interface

Select **Network** → **Link Aggregation** from the navigation tree. The **Summary** tab is displayed by default, as shown in a.

a. Display information of an aggregate interface

Summary	Create	Modify	Remove	
Aggregation Interface	Link Type	Partner ID	Selected Ports	Standby Ports
Bridge-Aggregation1	Static	0x8000,0000-0000-0000	0	3

2. Fields on the Summary tab

Field	Description
Aggregation interface	Type and ID of the aggregate interface. Bridge-Aggregation indicates a Layer 2 aggregate interface.
Link Type	Type of the aggregate interface, which can be static or dynamic.
Partner ID	ID of the remote device, including its LACP priority and MAC address.
Selected Ports	Number of Selected ports in each link aggregation group. Only Selected ports can transmit and receive user data.
Standby Ports	Number of Unselected ports in each link aggregation group. Unselected ports cannot transmit or receive user data.

Return to [Static aggregation group configuration task list](#).

Return to [Dynamic aggregation group configuration task list](#).

Setting LACP priority

Select **Network** → **LACP** from the navigation tree, and click the **Setup** tab to enter the page shown in a.

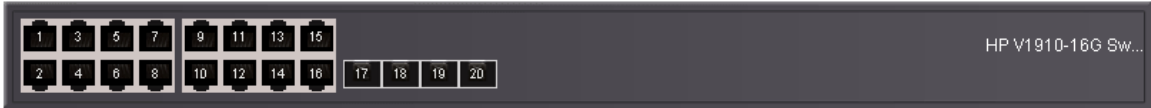
a. The Setup tab

Summary Setup




Select LACP enabled port(s) parameters :

Port Priority: (0-65535, Default = 32768)

Select port(s) to apply Port Priority:



Select All Select None

 Selected  LACP Enabled  LACP Disabled **Note:** Click a port to toggle its state between enabled and disabled.

Apply Cancel

Set global LACP parameters :

System Priority: (0-65535, Default = 32768)

Apply Cancel

After finishing each configuration item, click the right **Apply** button to submit the configuration.

2 describes the configuration items.

2. LACP priority configuration items

Item	Description
Select LACP enabled port(s) parameters	Set a port LACP priority.
Select port(s) to apply Port Priority	Select the ports where the port LACP priority you set will apply on the chassis front panel. You can set LACP priority not only on LACP-enabled ports but also on LACP-disabled ports.
System Priority	Set the LACP priority of the local system.

Return to [Dynamic aggregation group configuration task list](#).

Displaying information of LACP-enabled ports

Select **Network** → **LACP** from the navigation tree. The **Summary** tab is displayed by default, as shown in a.

a. Display information about LACP-enabled ports

Summary	Setup
---------	-------

Select port(s) from the table to view partner port details:

Unit	Port	LACP State	Port Priority	State	*Inactive Reason	Partner Port	Partner Port State	Oper Key
1	0/1	Enable	32768	Not in group	3	0	EF	1
1	0/2	Enable	32768	Not in group	3	0	EF	2

[View Details](#)

Partner Port Details:

Unit	Port	Partner ID	Partner Port Priority	Partner Oper Key
1	0/1	0x8000,0000-0000-0000	32768	0

*Note: The following numbers are used to indicate the reasons for being inactive.

- 1-- All active ports are already in-use for this aggregator.
- 2-- All aggregation resources are already in-use.
- 3-- The port is not configured properly.
- 4-- The port's partner is not configured properly.

The upper part of the page displays a list of all LACP-enabled ports on the device and information about them. To view information about the partner port of a LACP-enabled port, select it in the port list, and then click **View Details**. Detailed information about the peer port will be displayed on the lower part of the page.

2. Fields in the LACP-enabled port summary table

Field/button	Description
Unit	The ID of a device in a stack.
Port	Port where LACP is enabled.
LACP State	State of LACP on the port.
Port Priority	LACP priority of the port.

Field/button	Description
State	Active state of the port. If a port is selected, its state is active and the ID of the aggregation group it belongs to will be displayed.
Inactive Reason	Reason code indicating why a port is inactive (that is, unselected) for receiving/transmitting user data. For the meanings of the reason codes, see the bottom of the page shown in a .
Partner Port	Name of the peer port.
Partner Port State	<p>State information of the peer port, represented by letters A through H.</p> <ul style="list-style-type: none"> • A indicates that LACP is enabled. • B indicates that LACP short timeout has occurred. If B does not appear, it indicates that LACP long timeout has occurred. • C indicates that the link is considered as aggregatable by the sending system. • D indicates that the link is considered as synchronized by the sending system. • E indicates that the sending system considers that collection of incoming frames is enabled on the link. • F indicates that the sending system considers that distribution of outgoing frames is enabled on the link. • G indicates that the receive state machine of the sending system is using the default operational partner information. • H indicates that the receive state machine of the sending system is in the expired state.
Oper Key	Operational key of the local port

3 describes the fields in the **Partner Port Details** table

3. Fields in the Partner Port Details table

Field	Description
Unit	Number of the remote system
Port	Name of the remote port
Partner ID	LACP priority and MAC address of the remote system
Partner Port Priority	LACP priority of the remote port
Partner Oper Key	Operational key of the remote port.

Return to [Dynamic aggregation group configuration task list](#).

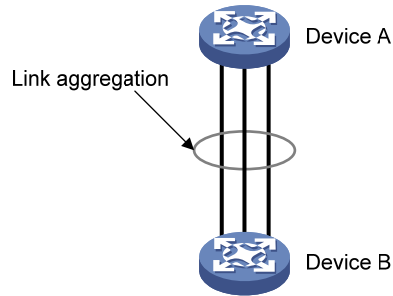
Link aggregation and LACP configuration example

Network requirements

As shown in [a](#), Switch A and Switch B are connected to each other through their Layer 2 Ethernet ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

Aggregate the ports on each device to form a link aggregation group, thus balancing incoming/outgoing traffic across the member ports.

a. Network diagram for static link aggregation configuration



Configuration procedure

You can create a static or dynamic link aggregation group to achieve load balancing.

Table 54 Approach 1: Create a static link aggregation group

Create static link aggregation group 1.

Select **Network** → **Link Aggregation** from the navigation tree, and click the **Create** tab to enter the page as shown in **b**.

b. Create static link aggregation group 1

Summary
Create
Modify
Remove

Enter Link Aggregation Interface ID: (1-10)

Specify Interface Type: Static (LACP Disabled) Dynamic (LACP Enabled)

Note: The type of the link aggregation interface set here overwrites the existing LACP settings of the ports in the link aggregation interface.

Select port(s) for the link aggregation interface:

1

3

5

7

9

11

13

15

17

18

19

20

HP V1910-16G Sw...

Select All
Select None

Selected Ports:

Members of the link aggregation interface to be created.

Unselected Ports:

Not a member of any link aggregation interface, and LACP is disabled on this port.

LACP has been enabled on this port.

Members of existing link aggregation interfaces.

Summary:

Aggregation Interface ID	Member Ports	Aggregation Interface Type
1	GE1/0/1-GE1/0/3	Static

Apply

Cancel

- Set the link aggregation interface ID to 1.

- Select the **Static (LACP Disabled)** option as the aggregate interface type.
- Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.
- Click **Apply**.

Table 55 Approach 2: Create a dynamic link aggregation group

Create dynamic link aggregation group 1.

Select **Network** → **Link Aggregation** from the navigation tree, and click the **Create** tab to enter the page as shown in c.

c. Create dynamic link aggregation group 1

Summary Create Modify Remove

Enter Link Aggregation Interface ID: (1-10)

Specify Interface Type: Static (LACP Disabled) Dynamic (LACP Enabled)

Note: The type of the link aggregation interface set here overwrites the existing LACP settings of the ports in the link aggregation interface.

Select port(s) for the link aggregation interface:

HP V1910-16G Sw...

Select All Select None

Selected Ports: Members of the link aggregation interface to be created.

Unselected Ports: Not a member of any link aggregation interface, and LACP is disabled on this port. LACP has been enabled on this port. Members of existing link aggregation interfaces.

Summary:

Aggregation Interface ID	Member Ports	Aggregation Interface Type
1	GE1/0/1-GE1/0/3	Dynamic

Apply Cancel

- Set the link aggregation interface ID to 1.
- Select the **Dynamic (LACP Enabled)** option as the aggregate interface type.
- Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.
- Click **Apply**.

Configuration guidelines

Follow these guidelines when configuring a link aggregation group:

- In an aggregation group, the port to be a selected port must be the same as the reference port in port attributes, and class-two configurations. To keep these configurations consistent, you should configure the port manually.
- Reference port: Select a port as the reference port from the ports that are in up state and with the same class-two configurations as the corresponding aggregate interface. The selection order is as follows: full duplex/high speed, full duplex/low speed, half duplex/high speed, and half duplex/low speed, with full duplex/high speed being the most preferred. If two ports with the same duplex mode/speed pair are present, the one with the lower port number wins out.
- Port attribute configuration includes the configuration of the port rate, duplex mode, and link state.
- For more information about class-two configurations, see [“Class-two configurations”](#).
- To guarantee a successful static aggregation, ensure that the ports at the two ends of each link to be aggregated are consistent in the Selected/Unselected state. To guarantee a successful dynamic aggregation, ensure that the peer ports of the ports aggregated at one end are also aggregated. The two ends can automatically negotiate the selected state of the ports.
- Removing a Layer 2 aggregate interface also removes the corresponding aggregation group. At the same time, all member ports leave the aggregation group.

LLDP configuration

Background

In a heterogeneous network, it is important that different types of network devices from different vendors can discover one other and exchange configuration for interoperability and management sake. To ensure compatibility, a standard configuration exchange platform was created.

The IETF drafted the Link Layer Discovery Protocol (LLDP) in IEEE 802.1AB. The protocol operates on the data link layer to exchange device information between directly connected devices. With LLDP, a device sends local device information as TLV (type, length, and value) triplets in LLDP Data Units (LLDPDUs) to the directly connected devices, and at the same time, stores the device information received in LLDPDUs sent from the LLDP neighbors in a standard management information base (MIB). It allows a network management system to quickly detect and identify Layer 2 network topology changes.

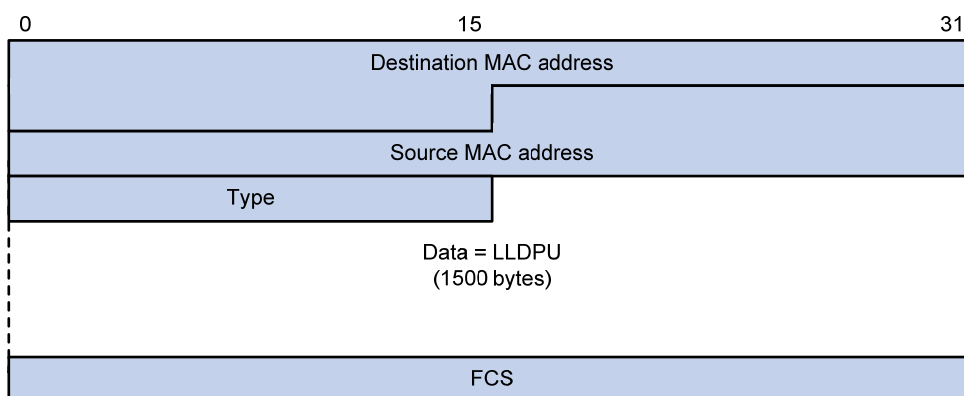
Basic concepts

LLDPDUs

LLDP sends device information in LLDPDUs. LLDPDUs are encapsulated in Ethernet II or Subnetwork Access Protocol (SNAP) frames.

Table 56 Ethernet II-encapsulated LLDPDU format

b. Ethernet II-encapsulated LLDPDU format



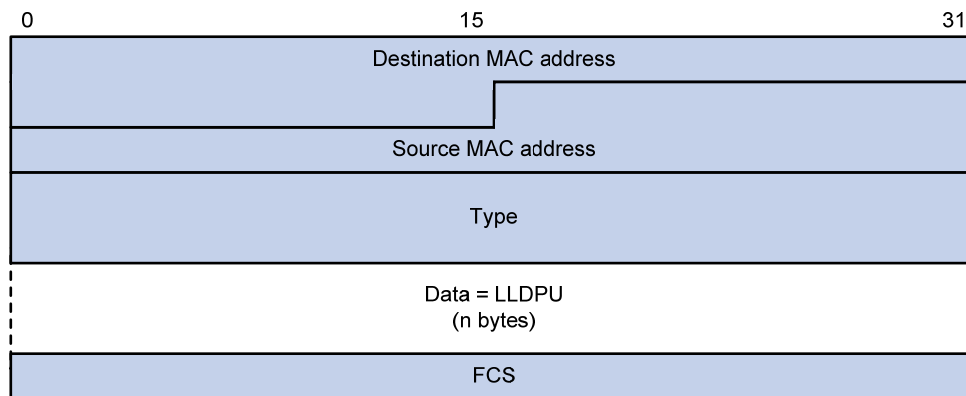
2. Fields in an Ethernet II encapsulated LLDPDU

Field	Description
Destination MAC address	The MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.
Source MAC address	The MAC address of the sending port. If the port does not have a MAC address, the MAC address of the sending bridge is used.
Type	The Ethernet type for the upper layer protocol. It is 0x88CC for LLDP.
Data	LLDPDU.

Field	Description
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

Table 57 SNAP-encapsulated LLDPDU format

b. SNAP-encapsulated LLDPDU format



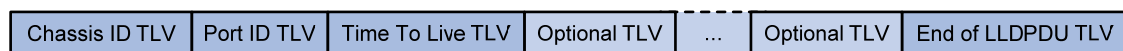
3. Fields in a SNAP encapsulated LLDPDU

Field	Description
Destination MAC address	The MAC address to which the LLDPDU is advertised. It is fixed to 0x0180-C200-000E, a multicast MAC address.
Source MAC address	The MAC address of the sending port. If the port does not have a MAC address, the MAC address of the sending bridge is used.
Type	The SNAP-encoded LLDP Ethernet type for the upper layer protocol. It is 0xAAAA-0300-0000-88CC for LLDP.
Data	LLDPDU.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

LLDPDU

LLDP uses LLDPDUs to exchange information. An LLDPDU comprises multiple TLV sequences. Each carries a specific type of device information, as shown in [a](#).

a. LLDPDU encapsulation format



An LLDPDU can carry up to 28 types of TLVs. Mandatory TLVs include Chassis ID TLV, Port ID TLV, Time To Live TLV, and End of LLDPDU TLV. Other TLVs are optional.

TLVs

TLVs are type, length, and value sequences that carry information elements. The type field identifies the type of information, the length field indicates the length of the information field in octets, and the value field contains the information itself.

LLDPDU TLVs fall into the following categories:

- Basic management TLVs
- Organizationally (IEEE 802.1 and IEEE 802.3) specific TLVs
- LLDP-MED (media endpoint discovery) TLVs

Basic management TLVs are essential to device management. Organizationally specific TLVs and LLDP-MED TLVs are used for enhanced device management; they are defined by standardization or other organizations and thus are optional to LLDPDUs.

Table 58 Basic management TLVs

2 lists the basic management TLV types. Some of them must be included in every LLDPDU.

2. Basic LLDP TLVs

Type	Description	Remarks
Chassis ID	Bridge MAC address of the sending device.	
Port ID	ID of the sending port. If the LLDPDU carries LLDP-MED TLVs, the port ID TLV carries the MAC address of the sending port or the bridge MAC in case the port does not have a MAC address. If the LLDPDU carries no LLDP-MED TLVs, the port ID TLV carries the port name.	Mandatory
Time To Live	Life of the transmitted information on the receiving device.	
End of LLDPDU	Marks the end of the TLV sequence in the LLDPDU.	
Port Description	Port description of the sending port.	
System Name	Assigned name of the sending device.	
System Description	Description of the sending device.	
System Capabilities	Identifies the primary functions of the sending device and the enabled primary functions.	Optional
Management Address	Management address used to reach higher level entities to assist discovery by network management, and the interface number and object identifier (OID) associated with the address.	

Table 59 IEEE 802.1 organizationally specific TLVs

3. IEEE 802.1 organizationally specific TLVs

Type	Description
Port VLAN ID	PVID of the sending port.
Port And Protocol VLAN ID	Port and protocol VLAN IDs.
VLAN Name	A specific VLAN name on the port.
Protocol Identity	Protocols supported on the port.

NOTE:

HP V1910 Switch Series can receive but cannot send protocol identity TLVs.

Table 60 IEEE 802.3 organizationally specific TLVs

4. IEEE 802.3 organizationally specific TLVs

Type	Description
MAC/PHY Configuration/Status	Contains the rate and duplex capabilities of the sending port, support for auto negotiation, enabling status of auto negotiation, and the current rate and duplex mode.
Power Via MDI	Contains Power supply capability of the port.
Link Aggregation	Indicates the support of the port for link aggregation, the aggregation capability of the port, and the aggregation status (whether the link is in an aggregation).
Maximum Frame Size	Indicates the supported maximum frame size. It is the MTU of the port.

LLDP-MED TLVs

LLDP-MED TLVs provide multiple advanced applications for voice over IP (VoIP), such as basic configuration, network policy configuration, and address and directory management. LLDP-MED TLVs provide a cost-effective and easy-to-use solution for deploying voice devices in Ethernet. LLDP-MED TLVs are shown in 1.

1. LLDP-MED TLVs

Type	Description
LLDP-MED Capabilities	Allows a MED endpoint to advertise the supported LLDP-MED TLVs and its device type.
Network Policy	Allows a network device or MED endpoint to advertise LAN type and VLAN ID of the specific port, and the Layer 2 and Layer 3 priorities for a specific set of applications.
Extended Power-via-MDI	Allows a network device or MED endpoint to advertise power-related information (according to IEEE 802.3AF).
Hardware Revision	Allows a MED endpoint device to advertise its hardware version.
Firmware Revision	Allows a MED endpoint to advertise its firmware version.
Software Revision	Allows a MED endpoint to advertise its software version.
Serial Number	Allows an LLDP-MED endpoint device to advertise its serial number.
Manufacturer Name	Allows a MED endpoint to advertise its vendor name.
Model Name	Allows a MED endpoint to advertise its model name.
Asset ID	Allows a MED endpoint to advertise its asset ID. The typical case is that the user specifies the asset ID for the endpoint to facilitate directory management and asset tracking.
Location Identification	Allows a network device to advertise the appropriate location identifier information for an endpoint to use in the context of location-based applications.

NOTE:

For more information about LLDPDU TLVs, see the IEEE standard (LLDP) 802.1AB-2005 and the LLDP-MED standard (ANSI/TIA-1057).

Management address

The management address of a device is used by the network management system to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV.

How LLDP works

Operating modes of LLDP

LLDP can operate in one of the following modes:

- TxRx mode. A port in this mode sends and receives LLDPDUs.
- Tx mode. A port in this mode only sends LLDPDUs.
- Rx mode. A port in this mode only receives LLDPDUs.
- Disable mode. A port in this mode does not send or receive LLDPDUs.

When the LLDP operating mode of a port changes, its LLDP protocol state machine re-initializes. A re-initialization delay, which is user configurable, prevents LLDP from being initialized too frequently during times of frequent operating mode change. With this delay configured, before a port can initialize LLDP, it must wait for the specified interval after the LLDP operating mode changes.

Transmitting LLDPDUs

An LLDP-enabled port operating in TxRx mode or Tx mode sends LLDPDUs to its directly connected devices both periodically and when the local configuration changes. A frame transmit interval between two successive LLDP frames prevents the network from being overwhelmed by LLDPDUs during times of frequent local device information change.

This interval is shortened to 1 second in either of the following cases:

- A new neighbor is discovered. A new LLDPDU is received carrying device information new to the local device.
- The LLDP operating mode of the port changes from Disable/Rx to TxRx or Tx.

This is the fast sending mechanism of LLDP. This feature sends a specific number of LLDPDUs at 1-second intervals to help LLDP neighbors discover the local device as soon as possible. Then, the normal LLDPDU transit interval resumes.

Receiving LLDPDUs

An LLDP-enabled port operating in TxRx mode or Rx mode checks the validity of TLVs carried in every received LLDPDU. If valid, the information is saved and an aging timer is set for it based on the time to live (TTL) value in the TTL TLV carried in the LLDPDU. If the TTL value is zero, the information is aged out immediately.

Compatibility of LLDP with CDP

To make your device work with Cisco IP phones, you must enable CDP compatibility.

If your LLDP-enabled device cannot recognize Cisco Discovery Protocol (CDP) packets, it does not respond to the requests of Cisco IP phones for the voice VLAN ID configured on the device. As a result, a requesting Cisco IP phone sends voice traffic without any tag to your device, which disables your device from differentiating the voice traffic from other types of traffic.

With CDP compatibility enabled, your device can receive and recognize CDP packets from a Cisco IP phone and respond with CDP packets, which carry the voice VLAN configuration TLVs. The voice traffic is confined in the configured voice VLAN, and differentiated from other types of traffic.

CDP-compatible LLDP operates in one of the following modes:

- TxRx: CDP packets can be transmitted and received.
- Disable: CDP packets cannot be transmitted or received.

Protocols and standards

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*

Configuring LLDP

LLDP configuration task list

Perform the tasks in 1 to configure LLDP:

1. LLDP configuration task list

Task	Remarks
Enabling LLDP on ports	Optional By default, LLDP is enabled on ports. Make sure that LLDP is also enabled globally, because LLDP can work on a port only when it is enabled both globally and on the port.
Configuring LLDP settings on ports	Optional LLDP settings include LLDP operating mode, packet encapsulation, CDP compatibility, device information polling, trapping, and advertised TLVs. By default, <ul style="list-style-type: none"> • The LLDP operating mode is TxRx. • The encapsulation format is Ethernet II. • CDP compatibility is disabled. • Device information polling and trapping are disabled. • All TLVs except the Location Identification TLV are advertised.
Configuring global LLDP setup	Required By default, global LLDP is disabled. To enable LLDP to work on a port, enable LLDP both globally and on the port.
Displaying LLDP information for a port	Optional You can display the local LLDP information, neighbor information, statistics, and status information of a port, where <ul style="list-style-type: none"> • The local LLDP information refers to the TLVs to be advertised by the local device to neighbors. • The neighbor information refers to the TLVs received from neighbors.

Task	Remarks
Displaying global LLDP information	Optional You can display the local global LLDP information and statistics.
Displaying LLDP information received from LLDP neighbors	Optional You can display the LLDP information received from LLDP neighbors.

NOTE:

LLDP-related configurations made in Ethernet interface view takes effect only on the current port, and those made in port group view takes effect on all ports in the current port group.

Enabling LLDP on ports

Select **Network** → **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in [a](#).

This tab displays the LLDP status and operating mode on a port. Select one or more ports and click **Enable** beneath the port list to enable LLDP on them.

To disable LLDP on a port, select the port and click **Disable**.

a. The Port Setup tab

Port Setup Global Setup Global Summary Neighbor Summary

Search Item: Port Name Keywords: Search

<input type="checkbox"/>	Port Name	LLDP Status	LLDP Work Mode	Operation
<input type="checkbox"/>	GigabitEthernet1/0/1	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/2	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/3	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/4	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/5	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/6	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/7	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/8	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/9	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/10	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/11	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/12	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/13	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/14	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/15	Enabled	TxRx	

20 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Enable Disable Modify Selected


Local Information Neighbor Information Statistic Information Status Information

Return to [LLDP configuration task list](#).

Configuring LLDP settings on ports

Select **Network** → **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in a.

You can configure LLDP settings on ports individually or in batch.

- To configure LLDP settings on individual ports, click the  icon for the port you are configuring. On the page displayed as shown in [a](#), you can modify or view the LLDP settings of the port.

a. The page for modifying LLDP settings on a port

Port Setup	Global Setup	Global Summary	Neighbor Summary
Interface Name	<input type="text" value="GigabitEthernet1/0/1"/>	LLDP State	<input type="text" value="Enable"/>
Basic Settings			
LLDP Operating Mode	<input type="text" value="TxRx"/>	Encapsulation Format	<input type="text" value="ETHII"/>
CDP Operating Mode	<input type="text" value="Disable"/>	LLDP Polling Interval	<input type="text"/> seconds (1-30)
LLDP Trapping	<input type="text" value="Disable"/>		
Base TLV Settings			
<input checked="" type="checkbox"/> Port Description	<input checked="" type="checkbox"/> System Capabilities		
<input checked="" type="checkbox"/> System Description	<input checked="" type="checkbox"/> System Name		
<input checked="" type="checkbox"/> Management Address	<input type="text"/>		
	<input type="text" value="Number"/>		
+Additional TLV Settings			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- To bulk configure LLDP settings on ports, select multiple ports and click **Modify Selected**. The page shown in [b](#) appears.

b. The page for modifying LLDP settings on ports in batch

Port Setup	Global Setup	Global Summary	Neighbor Summary
Interface Name GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3			
Basic Settings			
LLDP Operating Mode	<input type="text" value="TxRx"/>	Encapsulation Format	<input type="text" value="ETHII"/>
CDP Operating Mode	<input type="text" value="Disable"/>	LLDP Polling Interval	<input type="text"/> seconds(1-30)
LLDP Trapping	<input type="text" value="Disable"/>		
Base TLV Settings			
<input type="checkbox"/> Port Description	<input type="checkbox"/> System Capabilities		
<input type="checkbox"/> System Description	<input type="checkbox"/> System Name		
<input type="checkbox"/> Management Address	<input type="text"/>		
	<input type="text" value="String"/>		
+Additional Settings			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

2. Port LLDP configuration items

Item	Description
Interface Name	Displays the name of the port or ports you are configuring.
LLDP State	Displays the LLDP enabling status on the port you are configuring. This field is not available when you batch-configure ports.
LLDP Operating Mode	Set the LLDP operating mode on the port or ports you are configuring: <ul style="list-style-type: none"> • TxRx—Sends and receives LLDPDUs. • Tx—Sends but not receives LLDPDUs. • Rx—Receives but not sends LLDPDUs. • Disable—Neither sends nor receives LLDPDUs.
Basic Settings	Set the encapsulation for LLDPDUs: <ul style="list-style-type: none"> • ETHII—Encapsulates outgoing LLDPDUs in Ethernet II frames and processes an incoming LLDPDU only if its encapsulation is Ethernet II. • SNAP—Encapsulates outgoing LLDPDUs in Ethernet II frames and processes an incoming LLDPDU only if its encapsulation is Ethernet II.
Encapsulation Format	<ul style="list-style-type: none"> • SNAP—Encapsulates outgoing LLDPDUs in Ethernet II frames and processes an incoming LLDPDU only if its encapsulation is Ethernet II. <p>⚠ IMPORTANT: LLDP-CDP PDUs use only SNAP encapsulation.</p>

Item	Description	
CDP Operating Mode	<p>Set the CDP compatibility of LLDP:</p> <ul style="list-style-type: none"> • Disable—Neither sends nor receives CDPDUs. • TxRx—Sends and receives CDPDUs. <p>! IMPORTANT:</p> <p>To enable LLDP to be compatible with CDP on the port, you must enable CDP compatibility on the Global Setup tab and set the CDP operating mode on the port to TxRx.</p>	
LLDP Polling Interval	<p>Enable LLDP polling and set the polling interval.</p> <p>If no polling interval is set, LLDP polling is disabled.</p> <p>With the polling mechanism, LLDP periodically detects local configuration changes. If a configuration change is detected, an LLDPDU is sent to inform the LLDP neighbors of the change.</p>	
LLDP Trapping	<p>Set the enable status of the LLDP trapping function on the port or ports.</p> <p>LLDP trapping is used to report to the network management station critical events such as new neighbor devices detected and link failures.</p> <p>! IMPORTANT:</p> <p>To avoid excessive traps from being sent when topology is unstable, you can tune the minimum trap transit interval on the Global Setup tab.</p>	
Base TLV Settings	Port Description	Select to include the port description TLV in transmitted LLDPDUs.
	System Capabilities	Select to include the system capabilities TLV in transmitted LLDPDUs.
	System Description	Select to include the system description TLV in transmitted LLDPDUs.
	System Name	Select to include the system name TLV in transmitted LLDPDUs.
	Management Address	<p>Select to include the management address TLV in transmitted LLDPDUs and in addition, set the management address and its format (a numeric or character string in the TLV).</p> <p>If no management address is specified, the main IP address of the lowest VLAN carried on the port is used. If no main IP address is assigned to the VLAN, 127.0.0.1 is used.</p>
DOT1 TLV Setting	Port VLAN ID	Select to include the PVID TLV in transmitted LLDPDUs.
	Protocol VLAN ID	<p>Select to include port and protocol VLAN ID TLVs in transmitted LLDPDUs and specify the VLAN IDs to be advertised.</p> <p>If no VLAN is specified, the lowest protocol VLAN ID is transmitted.</p>
	VLAN Name	<p>Select to include VLAN name TLVs in transmitted LLDPDUs and specify the VLAN IDs to be advertised.</p> <p>If no VLAN is specified, the lowest VLAN carried on the port is advertised.</p>

Item	Description	
DOT3 TLV Setting	Link Aggregation	Select to include the link aggregation TLV in transmitted LLDPDUs.
	MAC/PHY Configuration/Status	Select to include the MAC/PHY configuration/status TLV in transmitted LLDPDUs.
	Maximum Frame Size	Select to include the maximum frame size TLV in transmitted LLDPDUs.
	Power via MDI	Select to include the power via MDI TLV in transmitted LLDPDUs.
MED TLV Setting	LLDP-MED Capabilities	Select to include the LLDP-MED capabilities TLV in transmitted LLDPDUs.
	Inventory	Select to include the hardware revision TLV, firmware revision TLV, software revision TLV, serial number TLV, manufacturer name TLV, model name TLV and asset ID TLV in transmitted LLDPDUs.
	Network Policy	Select to include the network policy TLV in transmitted LLDPDUs.
	Extended Power-via-MDI Capability	Select to include the extended power-via-MDI TLV in transmitted LLDPDUs.
	Emergency Number	Select to encode the emergency call number in the location identification TLV in transmitted LLDPDUs and set the emergency call number.
	Address	Select Address to encode the civic address information of the network connectivity device in the location identification TLV in transmitted LLDPDUs. In addition, set the device type, which can be a DHCP server, switch or LLDP-MED endpoint, country code, and network device address.
	Network Device Address	When configuring the network device address, select the address information type from the drop-down list, type the address information in the text box below and click Add next to the text box to add the information to the address information list below. To remove an address information entry, select the entry from the list, and click Delete . The civic address information can include language, province/state, country, city, street, house number, name, postal/zip code, room number, post office box, and if necessary, additional information.

Return to [LLDP configuration task list](#).

Configuring global LLDP setup

Select **Network** → **LLDP** from the navigation tree and click the **Global Setup** tab to enter the page shown in [a](#).

a. The Global Setup tab

Port Setup	Global Setup	Global Summary	Neighbor Summary
Global Setup			
LLDP Enable	Disable		
CDP Compatibility	Disable		
Fast LLDPDU Count	3	(1-10, Default = 3)	
TTL Multiplier	4	(2-10, Default = 4)	
Trap Interval	5	Second(5-3600, Default = 5)	
Reinit Delay	2	Second(1-10, Default = 2)	
Tx Delay	2	Second(1-8192, Default = 2)	
Tx Interval	30	Second(5-32768, Default = 30)	
<input type="button" value="Apply"/>			

2. Global LLDP setup configuration items

Item	Description
LLDP Enable	Select from the drop-down list to enable or disable global LLDP.
CDP Compatibility	<p>Select from the drop-down list to enable or disable CDP compatibility of LLDP.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> To enable LLDP to be compatible with CDP on a port, you must set the CDP work mode (or the CDP operating mode) on the port to TxRx in addition to enabling CDP compatibility on the Global Setup tab. As the maximum TTL allowed by CDP is 255 seconds, you must ensure that the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.
Fast LLDPDU Count	Set the number of LLDPDUs sent each time fast LLDPDU transmission is triggered.
TTL Multiplier	<p>Set the TTL multiplier.</p> <p>The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device. You can configure the TTL of locally sent LLDPDUs to determine how long information about the local device can be saved on a neighbor device by setting the TTL multiplier. The TTL is expressed as <i>TTL multiplier × LLDPDU transit interval</i>.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> If the product of the TTL multiplier and the LLDPDU transmit interval is greater than 65535, the TTL carried in transmitted LLDPDUs takes 65535 seconds. As the maximum TTL allowed by CDP is 255 seconds, you must ensure that the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.

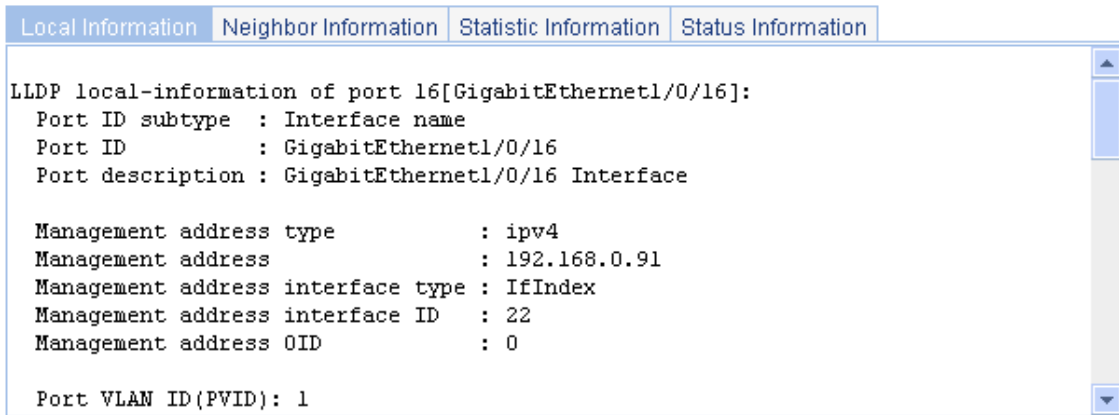
Item	Description
Trap Interval	<p>Set the minimum interval for sending traps.</p> <p>With the LLDP trapping function enabled on a port, traps are sent out the port to advertise the topology changes detected over the trap interval to neighbors. By tuning this interval, you can prevent excessive traps from being sent when topology is instable.</p>
Reinit Delay	<p>Set initialization delay for LLDP-enabled ports.</p> <p>Each time the LLDP operating mode of a port changes, its LLDP protocol state machine re-initializes. To prevent LLDP from being initialized too frequently at times of frequent operating mode change, initialization delay is introduced. With this delay mechanism, a port must wait for the specified interval before it can initialize LLDP after the LLDP operating mode changes.</p>
Tx Delay	<p>Set LLDPDU transmit delay.</p> <p>With LLDP enabled, a port advertises LLDPDUs to its neighbors both periodically and when the local configuration changes. To avoid excessive number of LLDPDUs caused by frequent local configuration changes, an LLDPDU transmit delay is introduced. Thus, after sending an LLDPDU, the port must wait for the specified interval before it can send another one.</p> <p>! IMPORTANT:</p> <p>LLDPDU transmit delay must be less than the TTL to ensure that the LLDP neighbors can receive LLDPDUs to update information about the device you are configuring before it is aged out.</p>
Tx Interval	<p>Set the LLDPDU transmit interval.</p> <p>! IMPORTANT:</p> <p>If the product of the TTL multiplier and the LLDPDU transmit interval is greater than 65535, the TTL carried in transmitted LLDPDUs takes 65535 seconds. In this case, the likelihood exists that the LLDPDU transmit interval is greater than TTL. You should avoid the situation, because the LLDP neighbors will fail to receive LLDPDUs to update information about the device you are configuring before it is aged out.</p>

Return to [LLDP configuration task list](#).

Displaying LLDP information for a port

Select **Network** → **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in [a](#). In the port list, click a port name to display its LLDP information at the lower half of the page. The LLDP information is organized by type and displayed in tabs as shown in [a](#). You can click these tabs to display data you are interested in.

a. The Local Information tab



2. Local information of an LLDP-enabled port

Field	Description
Port ID subtype	Port ID type: <ul style="list-style-type: none"> • Interface alias • Port component • MAC address • Network address • Interface name • Agent circuit ID • Locally assigned, namely, the local configuration
Power port class	The power over Ethernet port class: <ul style="list-style-type: none"> • PSE—A power supply device. • PD—A powered device.
Port power classification	Port power classification of the PD: <ul style="list-style-type: none"> • Unknown • Class 0 • Class 1 • Class 2 • Class 3 • Class 4
Media policy type	Available options include: <ul style="list-style-type: none"> • Unknown • Voice • Voice signaling • Guest voice • Guest voice signaling • Soft phone voice • Videoconferencing • Streaming video • Video signaling

Field	Description
PoE PSE power source	The type of PSE power source advertised by the local device: <ul style="list-style-type: none"> • Primary • Backup
Port PSE priority	Available options include: <ul style="list-style-type: none"> • Unknown—The PSE priority of the port is unknown. • Critical—The priority level 1. • High—The priority level 2. • Low—The priority level 3.

a. The Neighbor Information tab

Local Information
Neighbor Information
Statistic Information
Status Information

```

LLDP neighbor-information of port 16[GigabitEthernet1/0/16]:
Neighbor index      : 1
Update time        : 0 days,0 hours,39 minutes,0 seconds
Chassis type       : MAC address
Chassis ID         : 00e0-fc00-5502
Port ID type       : Interface name
Port ID            : GigabitEthernet1/0/23
Port description   : GigabitEthernet1/0/23 Interface
System name        : sysname
System description : Switch 4210G 24-Port Software Version 5.20 Release 2202P17
System capabilities supported : Bridge,Router

```

3. LLDP neighbor information of an LLDP-enabled port

Field	Description
Chassis type	Chassis ID type: <ul style="list-style-type: none"> • Chassis component • Interface alias • Port component • MAC address • Network address • Interface name • Locally assigned—Local configuration.
Chassis ID	Chassis ID depending on the chassis type, which can be a MAC address of the device.

Field	Description
Port ID type	Port ID type: <ul style="list-style-type: none"> • Interface alias • Port component • MAC address • Network address • Interface name • Agent circuit ID • Locally assigned—Local configuration.
Port ID	The port ID value.
System capabilities supported	The primary network function of the system: <ul style="list-style-type: none"> • Repeater • Bridge • Router
System capabilities enabled	The network function enabled on the system: <ul style="list-style-type: none"> • Repeater • Bridge • Router
Auto-negotiation supported	The support of the neighbor for auto negotiation.
Auto-negotiation enabled	The enable status of auto negotiation on the neighbor.
OperMau	Current speed and duplex mode of the neighbor.
Link aggregation supported	The neighbor supports link aggregation.
Link aggregation enabled	Link aggregation is enabled on the neighbor.
Aggregation port ID	Link aggregation group ID. It is 0 if the neighbor port is not assigned to any link aggregation group.
Maximum frame Size	The maximum frame size supported on the neighbor port.
Device class	MED device type: <ul style="list-style-type: none"> • Connectivity device—An intermediate device that provide network connectivity. • Class I—a generic endpoint device. All endpoints that require the discovery service of LLDP belong to this category. • Class II—A media endpoint device. The class II endpoint devices support the media stream capabilities in addition to the capabilities of generic endpoint devices. • Class III—A communication endpoint device. The class III endpoint devices directly support end users of the IP communication system. Providing all capabilities of generic and media endpoint devices, Class III endpoint devices are used directly by end users.

Field	Description
Media policy type	<p>Available options include:</p> <ul style="list-style-type: none"> • Unknown • Voice • Voice signaling • Guest voice • Guest voice signaling • Soft phone voice • Videoconferencing • Streaming video • Video signaling
Unknown Policy	Indicates whether or not the media policy type is unknown.
VLAN tagged	Indicates whether or not packets of the media VLAN are tagged.
Media policy VlanID	ID of the media VLAN.
Media policy L2 priority	Layer 2 priority.
Media policy Dscp	DSCP precedence.
HardwareRev	Hardware version of the neighbor.
FirmwareRev	Firmware version of the neighbor.
SoftwareRev	Software version of the neighbor.
SerialNum	The serial number advertised by the neighbor.
Manufacturer name	The manufacturer name advertised by the neighbor.
Model name	The model name advertised by the neighbor.
Asset tracking identifier	Asset ID advertised by the neighbor. This ID is used for the purpose of inventory management and asset tracking.
PoE PSE power source	<p>The type of PSE power source advertised by the neighbor:</p> <ul style="list-style-type: none"> • Primary • Backup
Port PSE priority	<p>Available options include:</p> <ul style="list-style-type: none"> • Unknown—The PSE priority of the port is unknown. • Critical—The priority level 1. • High—The priority level 2. • Low—The priority level 3.

a. The Statistic Information tab

Local Information	Neighbor Information	Statistic Information	Status Information
LLDP statistics information of port 10 [GigabitEthernet1/0/10]:			
The number of LLDP frames transmitted : 27			
The number of LLDP frames received : 66			
The number of LLDP frames discarded : 0			
The number of LLDP error frames : 65			
The number of LLDP TLVs discarded : 65			
The number of LLDP TLVs unrecognized : 0			
The number of LLDP neighbor information aged out : 1			
The number of CDP frames transmitted : 0			
The number of CDP frames received : 0			
The number of CDP frames discarded : 0			
The number of CDP error frames : 0			

Refresh

b. The Status Information tab

Local Information	Neighbor Information	Statistic Information	Status Information
Port 10 [GigabitEthernet1/0/10]:			
Port status of LLDP : Enable			
Admin status : Tx_Rx			
Trap flag : No			
Polling interval : 0s			
Number of neighbors: 2			
Number of MED neighbors : 0			
Number of CDP neighbors : 0			
Number of sent optional TLV : 22			
Number of received unknown TLV : 0			

Refresh

[Return to LLDP configuration task list.](#)

Displaying global LLDP information

Select **Network** → **LLDP** from the navigation tree, and click the **Global Summary** tab to display global local LLDP information and statistics, as shown in [a](#).

a. The Global Summary tab

Port Setup	Global Setup	Global Summary	Neighbor Summary
------------	--------------	----------------	------------------

Local Information

```

Global LLDP local-information:
Chassis ID      : 000f-e000-0002
System name     : HP V1910 Switch
System description : HP V1910-16G Switch Software Version 5.20 Alpha 1108
Copyright (c) 2004-2011 Hewlett-Packard Development Company, L.P.
System capabilities supported : Bridge,Router
System capabilities enabled   : Bridge,Router

MED information
Device class: Connectivity device

HardwareRev      : REV.B
FirmwareRev     : 138
    
```

Statistic Information

```

LLDP statistics global information:
LLDP neighbor information last change time:0 days,10 hours,47 minutes,39 seconds
The number of LLDP neighbor information inserted : 5
The number of LLDP neighbor information deleted  : 0
The number of LLDP neighbor information dropped  : 66
The number of LLDP neighbor information aged out : 0
    
```

Refresh

2. Global LLDP information

Field	Description
Chassis ID	The local chassis ID depending on the chassis type defined.
System capabilities supported	The primary network function advertised by the local device: <ul style="list-style-type: none"> • Bridge • Router
System capabilities enabled	The enabled network function advertised by the local device: <ul style="list-style-type: none"> • Bridge • Router

Field	Description
Device class	<p>The device class advertised by the local device:</p> <ul style="list-style-type: none"> Connectivity device—An intermediate device that provide network connectivity. Class I—A generic endpoint device. All endpoints that require the discovery service of LLDP belong to this category. Class II—A media endpoint device. The class II endpoint devices support the media stream capabilities in addition to the capabilities of generic endpoint devices. Class III—A communication endpoint device. The class III endpoint devices directly support end users of the IP communication system. Providing all capabilities of generic and media endpoint devices, Class III endpoint devices are used directly by end users.

Return to [LLDP configuration task list](#).

Displaying LLDP information received from LLDP neighbors

Select **Network** → **LLDP** from the navigation tree and click the **Neighbor Summary** tab to display the LLDP neighbor information, as shown in [a](#).

a. The Neighbor Summary tab

Update Time	Local Port	Chassis ID	Chassis ID Type	Port ID	Port ID Type	System Name*
0 days 0 hours 34 minutes 21 seconds	GigabitEthernet1/0/16	00e0-fc00-5502	MAC Address	GigabitEthernet1/0/23	Port Name	sysname
0 days 0 hours 39 minutes 0 seconds	GigabitEthernet1/0/16	00e0-fc00-5502	MAC Address	GigabitEthernet1/0/23	Port Name	sysname
0 days 0 hours 35 minutes 13 seconds	GigabitEthernet1/0/16	00e0-fc00-5502	MAC Address	GigabitEthernet1/0/23	Port Name	hp
0 days 0 hours 35 minutes 24 seconds	GigabitEthernet1/0/16	00e0-fc00-5502	MAC Address	GigabitEthernet1/0/23	Port Name	HP
0 days 1 hours 17 minutes 55 seconds	GigabitEthernet1/0/16	00e0-fc00-5502	MAC Address	GigabitEthernet1/0/23	Port Name	HP

9 records, 5 per page | page 1/2, record 1-5 | First Prev Next Last 1 GO

Refresh

Return to [LLDP configuration task list](#).

LLDP configuration examples

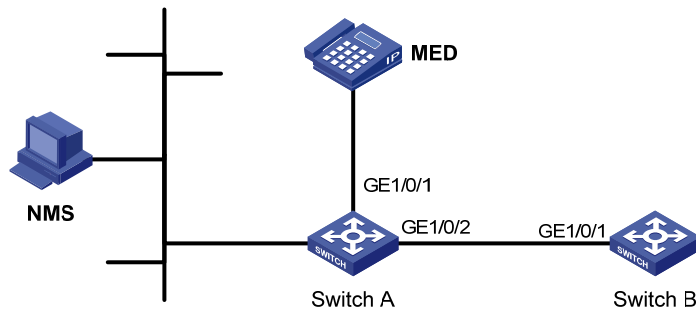
Basic LLDP configuration example

Network requirements

As shown in [a](#), the NMS and Switch A are located in the same Ethernet network. Switch A is connected to a MED device and Switch B through ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, respectively.

Enable LLDP on the ports of Switch A and Switch B to monitor the link between Switch A and Switch B and the link between Switch A and the MED device on the NMS.

a. Network diagram for basic LLDP configuration



Configuration procedure

Table 61 Configure Switch A

Enable LLDP on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. This step is optional, because LLDP is enabled on Ethernet ports by default.

Set the LLDP operating mode to Rx on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

- Select **Network** → **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in **b**. Select port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 and click **Modify Selected**. The page shown in **c** appears.

b. The Port Setup tab

Port Setup | Global Setup | Global Summary | Neighbor Summary

Search Item: Port Name | Keywords: | Search

<input type="checkbox"/>	Port Name	LLDP Status	LLDP Work Mode	Operation
<input checked="" type="checkbox"/>	GigabitEthernet1/0/1	Enabled	TxRx	
<input checked="" type="checkbox"/>	GigabitEthernet1/0/2	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/3	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/4	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/5	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/6	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/7	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/8	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/9	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/10	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/11	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/12	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/13	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/14	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/15	Enabled	TxRx	

20 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Enable | Disable | **Modify Selected**

Local Information | Neighbor Information | Statistic Information | Status Information

c. The page for setting LLDP on multiple ports

Port Setup	Global Setup	Global Summary	Neighbor Summary
Interface Name		GigabitEthernet1/0/1 GigabitEthernet1/0/2	
Basic Settings			
LLDP Operating Mode	Rx	Encapsulation Format	ETHII
CDP Operating Mode	Disable	LLDP Polling Interval	seconds(1-30)
LLDP Trapping	Disable		
Base TLV Settings			
<input type="checkbox"/> Port Description	<input type="checkbox"/> System Capabilities		
<input type="checkbox"/> System Description	<input type="checkbox"/> System Name		
<input type="checkbox"/> Management Address			
			String
+Additional Settings			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- Select **Rx** from the **LLDP Operating Mode** drop-down list.
 - Click **Apply**.
- # Enable global LLDP.
- Click the **Global Setup** tab, as shown in d.

d. The Global Setup tab

Port Setup	Global Setup	Global Summary	Neighbor Summary
------------	---------------------	----------------	------------------

Global Setup

LLDP Enable	Enable	▼
CDP Compatibility	Disable	▼
Fast LLDPDU Count	3	(1-10, Default = 3)
TTL Multiplier	4	(2-10, Default = 4)
Trap Interval	5	Second(5-3600, Default = 5)
Reinit Delay	2	Second(1-10, Default = 2)
Tx Delay	2	Second(1-8192, Default = 2)
Tx Interval	30	Second(5-32768, Default = 30)


Apply

- Select **Enable** from the **LLDP Enable** drop-down list.
- Click **Apply**.

Table 62 Configure Switch B

Enable LLDP on port GigabitEthernet 1/0/1. (Optional. By default, LLDP is enabled on Ethernet ports.)






Set the LLDP operating mode to Tx on GigabitEthernet 1/0/1.

- Select **Network** → **LLDP** from the navigation tree to enter the **Port Setup** tab, as shown in e. Click the  icon for port GigabitEthernet 1/0/1. The page shown in f is displayed.

e. The Port Setup tab

Port Setup	Global Setup	Global Summary	Neighbor Summary
------------	--------------	----------------	------------------

► Search Item: Port Name ▼ Keywords: Search

<input type="checkbox"/>	Port Name	LLDP Status	LLDP Work Mode	Operation
<input type="checkbox"/>	GigabitEthernet1/0/1	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/2	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/3	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/4	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/5	Enabled	TxRx	

f. The page for configuring LLDP on the selected port

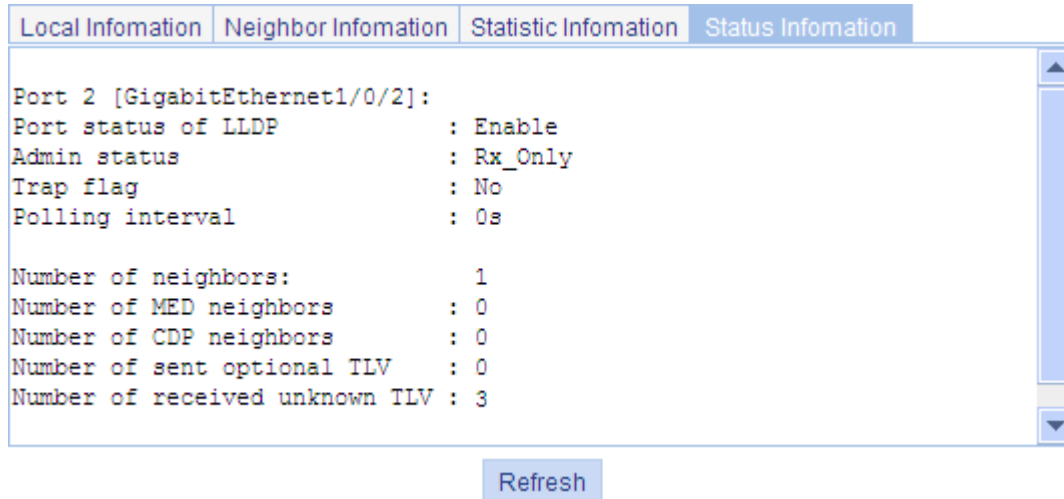
Port Setup	Global Setup	Global Summary	Neighbor Summary	
Interface Name	GigabitEthernet1/0/1	LLDP State	Enable	
Basic Settings				
LLDP Operating Mode	Tx	Encapsulation Format	ETHII	
CDP Operating Mode	Disable	LLDP Polling Interval		seconds (1-30)
LLDP Trapping	Disable			
Base TLV Settings				
<input checked="" type="checkbox"/> Port Description		<input checked="" type="checkbox"/> System Capabilities		
<input checked="" type="checkbox"/> System Description		<input checked="" type="checkbox"/> System Name		
<input checked="" type="checkbox"/> Management Address				
				Number
+ Additional TLV Settings				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

- Select **Tx** from the **LLDP Operating Mode** drop-down list.
 - Click **Apply**.
- # Enable global LLDP and configure the global LLDP setup as needed (see d).
- Click the **Global Setup** tab.
 - Select **Enable** from the **LLDP Enable** drop-down list.
 - Click **Apply**.

Configuration verification

- # Display the status information of port GigabitEthernet 1/0/2 on Switch A.
- Select **Network** → **LLDP** from the navigation tree to enter the **Port Setup** tab.
 - Click **GigabitEthernet1/0/2** in the port list.
 - Click the **Status Information** tab at the lower half of the page. The output shows that port GigabitEthernet 1/0/2 is connected to a non-MED neighbor device (Switch B), as shown in a.

a. The Status Information tab



The screenshot shows a network configuration interface with four tabs: Local Information, Neighbor Information, Statistic Information, and Status Information. The Status Information tab is active, displaying the following text:

```
Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP      : Enable
Admin status             : Rx_Only
Trap flag                 : No
Polling interval         : 0s

Number of neighbors:      1
Number of MED neighbors  : 0
Number of CDP neighbors  : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 3
```

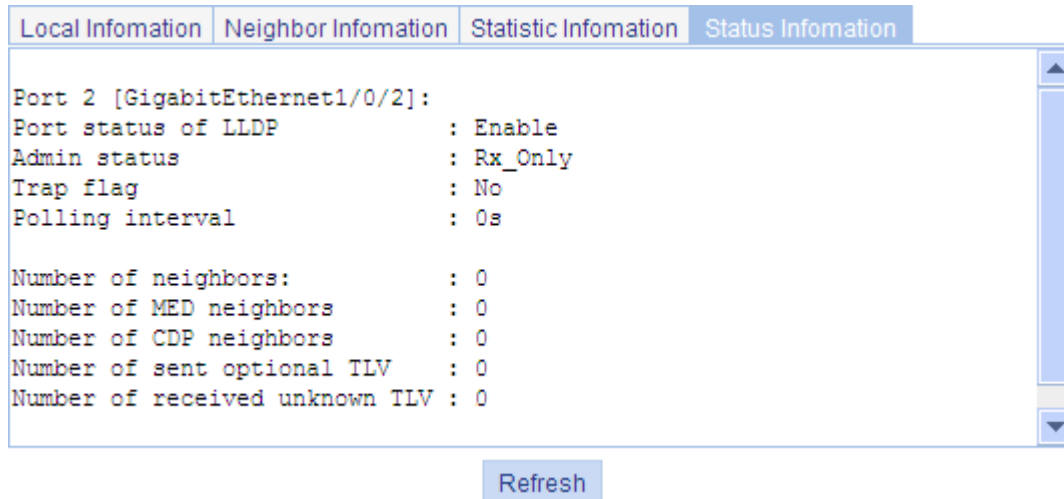
Below the text is a blue button labeled "Refresh".

Tear down the link between Switch A and Switch B.

Display the status information of port GigabitEthernet 1/0/2 on Switch A.

- Click **Refresh**. The updated status information of port GigabitEthernet 1/0/2 shows that no neighbor device is connected to the port, as shown in b.

b. The Status Information tab displaying the updated port status information



The screenshot shows the same network configuration interface as in part a, but with the following text displayed in the Status Information tab:

```
Port 2 [GigabitEthernet1/0/2]:
Port status of LLDP      : Enable
Admin status             : Rx_Only
Trap flag                 : No
Polling interval         : 0s

Number of neighbors:      : 0
Number of MED neighbors  : 0
Number of CDP neighbors  : 0
Number of sent optional TLV : 0
Number of received unknown TLV : 0
```

Below the text is a blue button labeled "Refresh".

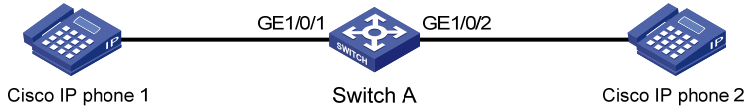
CDP-compatible LLDP configuration example

Network requirements

As shown in a, port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Switch A are each connected to a Cisco IP phone.

On Switch A, configure VLAN 2 as a voice VLAN and enable CDP compatibility of LLDP to allow the Cisco IP phones to automatically configure the voice VLAN, confining their voice traffic within the voice VLAN to be isolated from other types of traffic.

a. Network diagram for CDP-compatible LLDP configuration



Configuration procedure

Create VLAN 2.

- Select **Network** → **VLAN** from the navigation bar and click the **Create** tab to enter the page shown in a.

a. The page for creating VLANs

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove
-------------	---------------	-------------	--------	-------------	-------------	--------

Create:

VLAN IDs: Example:3, 5-10

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID	Description
<input type="text"/>	<input type="text" value=""/> (1-32 Chars.)

- Type **2** in the **VLAN IDs** field.
- Click **Create**.

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 as trunk ports.

- Select **Device** → **Port Management** from the navigation bar and click the **Setup** tab to enter the page shown in b.

b. The page for configuring ports

Summary Detail **Setup**

Basic Configuration

Port State Speed Duplex

Link Type PVID (1-4094)

Advanced Configuration


MDI Flow Control

Power Save Max MAC Count (0-8192)

Storm Suppression

Broadcast Suppression Multicast Suppression Unicast Suppression

pps range (1-148810 for a 100 Mbps port, 1-1488100 for a GE port, and 1-14881000 for a 10GE port)
kpps range (1-102400 for a 100 Mbps port, 1-1024000 for a GE port, and 1-10240000 for a 10GE port)

 HP V1910-16G Sw...

Unit

Unit	Selected Ports
1	GE1/0/1-GE1/0/2

• It may take some time if you apply the above settings to multiple ports.

- Select **Trunk** in the **Link Type** drop-down list.
 - Select port GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on the chassis front panel.
 - Click **Apply**.
- # Configure the voice VLAN function on the two ports.
- Select **Network** → **Voice VLAN** from the navigation bar and click the **Port Setup** tab to enter the page shown in [c](#).

c. The page for configuring the voice VLAN function on ports

The screenshot shows a configuration page with tabs: Summary, Setup, Port Setup (selected), OUI Summary, OUI Add, and OUI Remove. The 'Voice VLAN port mode' is set to 'Auto', 'Voice VLAN port state' is 'Enable', and 'Voice VLAN ID' is '2' (with a range of 2-4094). Below, a 'Select ports' section shows a grid of 20 ports (1-20) on a chassis front panel. Ports 1 and 2 are selected. Below the grid are 'Select All' and 'Select None' buttons. A text box shows 'Ports selected for voice VLAN: GE1/0/1-GE1/0/2'. At the bottom right, 'Apply' and 'Cancel' buttons are visible.

- Select **Auto** in the **Voice VLAN port mode** drop-down list.
- Select **Enable** in the **Voice VLAN port state** drop-down list.
- Type **2** in the **Voice VLAN ID** field.
- Select ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on the chassis front panel.
- Click **Apply**.

Enable LLDP on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. If LLDP is enabled (the default setting), skip this step.

Set both the LLDP operating mode and the CDP operating mode to TxRx on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

- Select **Network** → **LLDP** from the navigation tree to enter the **Port Setup** tab. Select ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 and click **Modify Selected**, as shown in d. The page shown in e is displayed.

d. The Port Setup tab

Port Setup | Global Setup | Global Summary | Neighbor Summary

Search Item: Port Name | Keywords: | Search

<input type="checkbox"/>	Port Name	LLDP Status	LLDP Work Mode	Operation
<input checked="" type="checkbox"/>	GigabitEthernet1/0/1	Enabled	TxRx	
<input checked="" type="checkbox"/>	GigabitEthernet1/0/2	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/3	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/4	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/5	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/6	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/7	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/8	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/9	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/10	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/11	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/12	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/13	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/14	Enabled	TxRx	
<input type="checkbox"/>	GigabitEthernet1/0/15	Enabled	TxRx	

20 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

Enable | Disable | **Modify Selected**

Local Information | Neighbor Information | Statistic Information | Status Information

e. The page for modifying LLDP settings on ports

Port Setup	Global Setup	Global Summary	Neighbor Summary
Interface Name	GigabitEthernet1/0/1 GigabitEthernet1/0/2		
Basic Settings			
LLDP Operating Mode	TxRx	Encapsulation Format	ETHII
CDP Operating Mode	TxRx	LLDP Polling Interval	seconds (1-30)
LLDP Trapping	Disable		
Base TLV Settings			
<input type="checkbox"/> Port Description	<input type="checkbox"/> System Capabilities		
<input type="checkbox"/> System Description	<input type="checkbox"/> System Name		
<input type="checkbox"/> Management Address			
			String
+Additional Settings			
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- Select **TxRx** from the **LLDP Operating Mode** drop-down list.
 - Select **TxRx** from the **CDP Operating Mode** drop-down list.
 - Click **Apply**.
- # Enable global LLDP and CDP compatibility of LLDP.
- Click the **Global Setup** tab, as shown in f.

f. The Global Setup tab

Port Setup	Global Setup	Global Summary	Neighbor Summary
Global Setup			
LLDP Enable	Enable		
CDP Compatibility	Enable		
Fast LLDPDU Count	3	(1-10, Default = 3)	
TTL Multiplier	4	(2-10, Default = 4)	
Trap Interval	5	Second(5-3600, Default = 5)	
Reinit Delay	2	Second(1-10, Default = 2)	
Tx Delay	2	Second(1-8192, Default = 2)	
Tx Interval	30	Second(5-32768, Default = 30)	
<input type="button" value="Apply"/>			

- Select **Enable** from the **LLDP Enable** drop-down list.
- Select **Enable** from the **CDP Compatibility** drop-down list.
- Click **Apply**.

Configuration verification

Display information about LLDP neighbors on Switch A.

Display information about LLDP neighbors on Switch A after completing the configuration. You can see that Switch A has discovered the Cisco IP phones attached to ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 and obtained their device information.

Configuration guidelines

When configuring LLDP, follow these guidelines:

Table 63 To make LLDP take effect, you must enable it both globally and on ports.

Table 64 When selecting TLVs to send in LLDPDUs, note the following:

- To advertise LLDP-MED TLVs, you must include the LLDP-MED capabilities set TLV.
- To remove the LLDP-MED capabilities set TLV, you must remove all other LLDP-MED TLVs.
- To remove the MAC/PHY configuration TLV, remove the LLDP-MED capabilities set TLV first.
- If the LLDP-MED capabilities set TLV is included, the MAC/PHY configuration/status TLV is included automatically.

IGMP snooping configuration

Overview

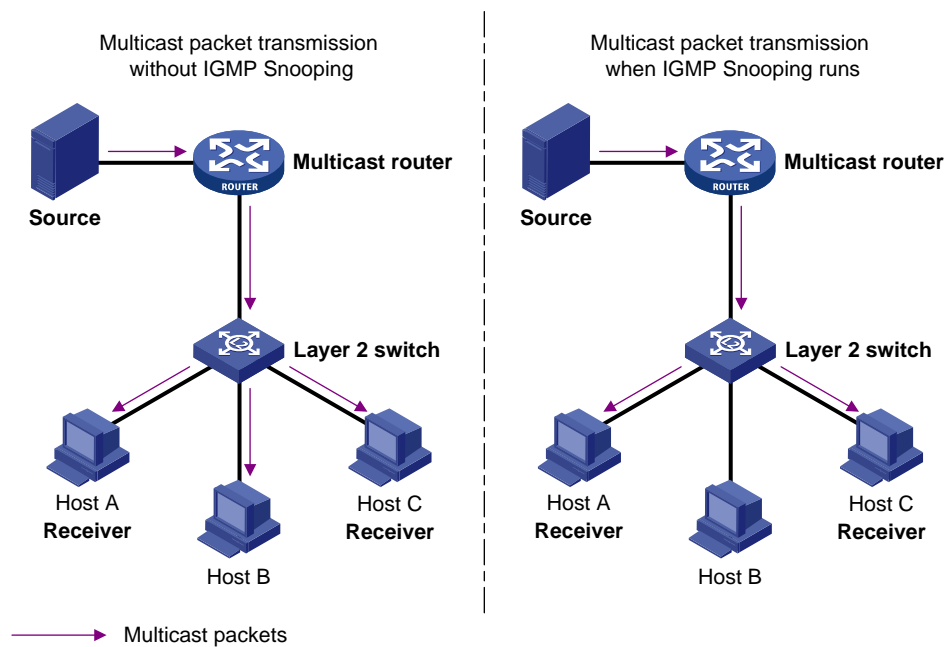
Internet Group Management Protocol (IGMP) snooping is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

Principle of IGMP snooping

By analyzing received IGMP messages, a Layer 2 device running IGMP snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

As shown in a, when IGMP snooping is not running on the switch, multicast packets are flooded to all devices at Layer 2. However, when IGMP snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2.

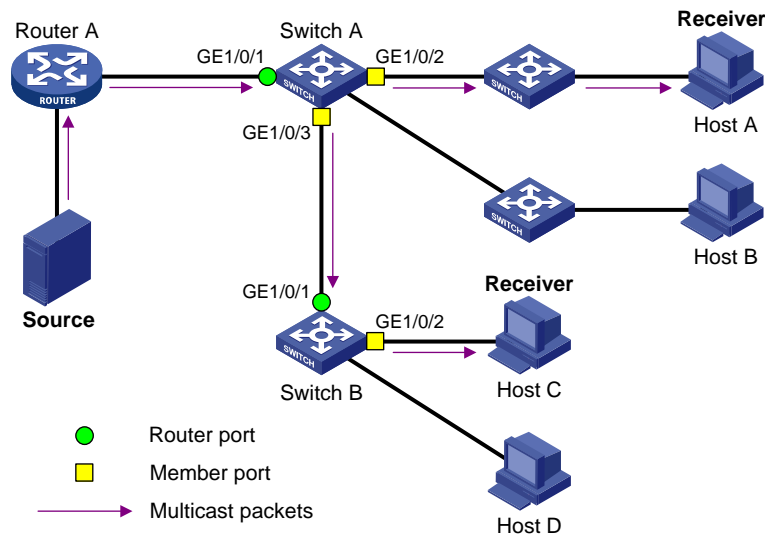
a. Multicast forwarding before and after IGMP snooping runs



IGMP snooping related ports

As shown in a, Router A connects to the multicast source, IGMP snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (namely, multicast group members).

a. IGMP snooping related ports



IGMP snooping related ports include:

- Router port: A router port is a port on an Ethernet switch that leads the switch towards the Layer 3 multicast device (DR or IGMP querier). In the figure, GigabitEthernet 1/0/1 of Switch A and GigabitEthernet 1/0/1 of Switch B are router ports. A switch registers all its local router ports in its router port list.
- Member port: On an Ethernet switch, a member port (also known as multicast group member port) connects the switch to a multicast group member. In the figure, GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 of Switch A and GigabitEthernet 1/0/2 of Switch B are member ports. A switch registers all its member ports in the IGMP snooping forwarding table.

NOTE:

- In this document, a router port is a port on the switch that leads the switch to a Layer 3 multicast device, rather than a port on a router.
 - Unless otherwise specified, router ports and member ports in this document consist of dynamic and static ports.
 - An IGMP snooping enabled switch deems that all its ports on which IGMP general queries with the source address other than 0.0.0.0 or PIM hello messages are received to be router ports.
-

Work mechanism of IGMP snooping

A switch running IGMP snooping performs different actions when it receives different IGMP messages, as follows:

⚠ CAUTION:

You can add or delete only dynamic ports rather than static ports.

When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers (224.0.0.1) on the local subnet to find out whether any active multicast group members exist on the subnet.

After receiving an IGMP general query, the switch forwards it through all ports in the VLAN except the receiving port and performs the following to the receiving port:

- The switch resets the aging timer for the receiving port if the port is in the router port list.
- The switch adds the receiving port to the router port list if it is not in the list and starts the aging timer for the port.

When receiving a membership report

A host sends an IGMP membership report to the IGMP querier in the following circumstances:

- After receiving an IGMP query, a multicast group member host responds with an IGMP report.
- When intended to join a multicast group, a host sends an IGMP report to the querier to announce its interest in the multicast information addressed to that group.

After receiving an IGMP report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported multicast group, and performs the following:

- If no forwarding table entry exists for the reported group, the switch creates an entry, adds the port as a member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported group, but the port is not included in the outgoing port list, the switch adds the port as a member port to the outgoing port list, and starts a member port aging timer for that port.
- If a forwarding table entry exists for the reported group and the port is not included in the outgoing port list, the switch resets the member port aging timer for that port.

NOTE:

A switch does not forward an IGMP report through a non-router port. If the switch forwards a report message through a member port, all the attached hosts listening to the reported multicast address will suppress their own reports after hearing this report according to the IGMP report suppression mechanism on them. This will prevent the switch from knowing whether any hosts attached to that port are still active members of the reported multicast group.

When receiving a leave group message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, so the switch cannot know immediately that the host has left the multicast group. However, as the host stops sending IGMP membership reports as soon as it leaves a multicast group, the switch deletes the forwarding entry for the member port corresponding to the host from the forwarding table when its aging timer expires.

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave message to the multicast router to announce that it has left the multicast group. When the switch receives a group-specific IGMP leave group message on a member port, it first checks whether a forwarding table entry for that group exists, and, if one exists, whether its outgoing port list contains that port.

- If the forwarding table entry does not exist or if the outgoing port list does not contain the port, the switch discards the IGMP leave group message instead of forwarding it to any port.
- If the forwarding table entry exists and the outgoing port list contains the port, the switch forwards the IGMP leave group message to the router ports in the VLAN. Because the switch does not know whether any other member hosts for that group still exist under the port from which the leave message arrived, the switch does not immediately remove the port from the outgoing port list. Instead, the switch resets the member port aging timer for that port.

After receiving the IGMP leave group message from a host, the IGMP querier resolves from the message the address of the multicast group that the host just left and sends an IGMP group-specific query to that multicast group through the port that received the leave group message. After hearing the IGMP group-specific query, the switch forwards it through all its router ports in the VLAN and all member ports for that multicast group, and performs the following to the port before the member port aging timer of the port expires (in case it is a dynamic member port):

- If any IGMP report in response to the group-specific query is heard on a member port before its aging timer expires, this means that some host attached to the port is receiving or expecting to receive multicast data for that multicast group. The switch resets the aging timer of the member port.
- If no IGMP report in response to the group-specific query is heard on a member port before its aging timer expires, this means that no hosts attached to the port are still listening to that group address. The switch removes the port from the outgoing port list of the forwarding table entry for that multicast group when the aging timer expires.

IGMP snooping querier

In an IP multicast network running IGMP, a multicast router or Layer 3 multicast switch is responsible for sending IGMP general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer. This router or Layer 3 switch is called an IGMP querier.

However, a Layer 2 multicast switch does not support IGMP, and therefore cannot send general queries by default. By enabling IGMP snooping on a Layer 2 switch in a VLAN where multicast traffic needs to be Layer-2 switched only and no multicast routers are present, the Layer 2 switch will act as the IGMP snooping querier to send IGMP queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

Protocols and standards

- RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

Configuring IGMP snooping

Configuration task list

Task	Remarks
Enabling IGMP snooping globally	Required Disabled by default.

Task	Remarks
Configuring IGMP snooping in a VLAN	<p>Required</p> <p>Enable IGMP snooping in the VLAN and configure the IGMP snooping version and querier feature.</p> <p>By default, IGMP snooping is disabled in a VLAN.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> IGMP snooping must be enabled globally before it can be enabled in a VLAN. When you enable IGMP snooping in a VLAN, this function takes effect for ports in this VLAN only.
Configuring IGMP snooping port functions	<p>Optional</p> <p>Configure the maximum number of multicast groups allowed and the fast leave function for ports in the specified VLAN.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> IGMP snooping must be enabled globally before IGMP snooping can be enabled on a port. IGMP snooping configured on a port takes effect only after IGMP snooping is enabled in the VLAN.
Display IGMP snooping multicast entry information	Optional

Enabling IGMP snooping globally

Select **Network** → **IGMP Snooping** in the navigation tree to enter the basic configuration page shown in a.

a. Basic IGMP snooping configurations

Basic

Advanced

IGMP Snooping: Enable Disable [Apply](#)

VLAN Configuration

▶ Search Item: Keywords: [Search](#)

VLAN ID	IGMP Snooping	Version	Drop Unknown	Querier	Query Interval (Sec)	GeneralQuery SourceIP	SpecialQuery SourceIP	Operation
1	Disabled	2	Disabled	Disabled	60	0.0.0.0	0.0.0.0	
999	Enabled	2	Disabled	Disabled	60	1.1.1.1	1.1.1.2	


[+ Show Entries](#)

2. IGMP snooping configuration items

Item	Description
IGMP snooping	Globally enable or disable IGMP snooping.

Return to [Configuration task list](#).

Configuring IGMP snooping in a VLAN

Select **Network** → **IGMP Snooping** in the navigation tree to enter the basic configuration page shown in [a](#). Click the  icon corresponding to the VLAN to enter the page you can configure IGMP snooping in the VLAN, as shown in [a](#).

a. VLAN configuration

Basic Advanced

VLAN Configuration

VLAN ID:	1
IGMP Snooping:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Version:	<input checked="" type="radio"/> 2 <input type="radio"/> 3
Drop Unknown:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Querier:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Query Interval:	<input type="text" value="60"/> *Seconds (2-300, Default = 60)
General Query Source IP:	<input type="text" value="0.0.0.0"/> *IP Address
Special Query Source IP:	<input type="text" value="0.0.0.0"/> *IP Address

Items marked with an asterisk(*) are required

2. Items for configuring IGMP snooping in a VLAN

Item	Description
VLAN ID	This field displays the ID of the VLAN to be configured.
IGMP Snooping	Enable or disable IGMP snooping in the VLAN. You can proceed with the subsequent configurations only if Enable is selected here.
Version	By configuring an IGMP snooping version, you actually configure the versions of IGMP messages that IGMP snooping can process. <ul style="list-style-type: none">IGMP snooping version 2 can process IGMPv1 and IGMPv2 messages, but not IGMPv3 messages, which will be flooded in the VLAN.IGMP snooping version 3 can process IGMPv1, IGMPv2, and IGMPv3 messages.

Item	Description
Drop Unknown	<p>Enable or disable the function of dropping unknown multicast packets.</p> <p>Unknown multicast data refer to multicast data for which no entries exist in the IGMP snooping forwarding table.</p> <ul style="list-style-type: none"> • With the function of dropping unknown multicast data enabled, the switch drops all the unknown multicast data received. • With the function of dropping unknown multicast data disabled, the switch floods unknown multicast data in the VLAN to which the unknown multicast data belong.
Querier	<p>Enable or disable the IGMP snooping querier function.</p> <p>On a network without Layer 3 multicast devices, no IGMP querier-related function can be implemented because a Layer 2 device does not support IGMP. To address this issue, you can enable IGMP snooping querier on a Layer 2 device so that the device can generate and maintain multicast forwarding entries at data link layer, thereby implementing IGMP querier-related functions.</p>
Query interval	Configure the IGMP query interval.
General Query Source IP	Specify the source IP address of general queries. HP recommends you to configure a non-all-zero IP address as the source IP address of IGMP queries.
Special Query Source IP	Specify the source IP address of group-specific queries. HP recommends you to configure a non-all-zero IP address as the source IP address of IGMP queries.

Return to [Configuration task list](#).

Configuring IGMP snooping port functions

Select **Network** → **IGMP Snooping** in the navigation tree to enter the basic configuration page and then click the **Advanced** tab to enter the page shown in a.

a. Advanced configuration

Basic

Advanced

Port Configuration

Port:

VLAN ID: *(1-4094, example: 3,5-10) Up to 10 VLAN ranges can be specified.

Multicast Group Limit: (1-255)

Fast Leave: Enable Disable

Items marked with an asterisk(*) are required

► Search Item: Keywords:


VLAN ID	Multicast Group Limit	Fast Leave	Operation
---------	-----------------------	------------	-----------

2. Configuration items for advanced IGMP snooping features

Item	Description
Port	<p>Select the port on which advanced IGMP snooping features are to be configured. The port can be an Ethernet port or Layer-2 aggregate port.</p> <p>After a port is selected, advanced features configured on this port are displayed at the lower part of this page.</p> <p>⚠ IMPORTANT:</p> <p>Advanced IGMP snooping features configured on a Layer 2 aggregate port do not interfere with features configured on its member ports, nor do they take part in aggregation calculations; features configured on a member port of the aggregate group will not take effect until it leaves the aggregate group</p>
VLAN ID	<p>Specify a VLAN in which you can configure the fast leave function for the port or the maximum number of multicast groups allowed on the port.</p> <p>Configurations made in a VLAN take effect for the ports in this VLAN only.</p>
Group Limit	<p>Configure the maximum number of multicast groups that the port can join.</p> <p>With this feature, you can regulate multicast traffic on the port.</p> <p>⚠ IMPORTANT:</p> <p>When the number of multicast groups a port has joined reaches the configured threshold, the system deletes all the forwarding entries persistent on that port from the IGMP snooping forwarding table, and the hosts on this port need to join the multicast groups again.</p>
Fast Leave	<p>Enable or disable the fast leave function for the port.</p> <p>With the fast leave function enabled on a port, the switch, when receiving an IGMP leave message on the port, immediately deletes that port from the outgoing port list of the corresponding forwarding table entry. Then, when receiving IGMP group-specific queries for that multicast group, the switch does not forward them to that port. In VLANs where only one host is attached to each port, the fast leave function helps improve bandwidth and resource usage.</p> <p>⚠ IMPORTANT:</p> <p>If fast leave is enabled for a port to which more than one host is attached, when one host leaves a multicast group, the other hosts listening to the same multicast group fails to receive multicast data.</p>

Return to [Configuration task list](#).

Display IGMP snooping multicast entry information

Select **Network** → **IGMP Snooping** in the navigation tree to enter the basic configuration page shown in [a](#). Click the plus sign (+) in front of **Show Entries** to display information about IGMP snooping multicast entries, as shown in [a](#). You can view the detailed information of an entry by clicking the  icon corresponding to the entry.

a. Display entry information

Show Entries

Search Item: **VLAN ID** Keywords: Search

VLAN ID	Source	Group	Operation
100	0.0.0.0	224.1.1.1	

b. Information about an IGMP snooping multicast entry

Entry Details

VLAN ID:	100
Source Address:	0.0.0.0
Group Address:	224.1.1.1
Router Port(s):	GigabitEthernet1/0/1
Member Port(s):	GigabitEthernet1/0/3

[Back](#)

2. Description of IGMP snooping multicast entries

Item	Description
VLAN ID	ID of the VLAN to which the entry belongs
Source Address	Multicast source address, where 0.0.0.0 indicates all multicast sources.
Group Address	Multicast group address
Router Port(s)	All router ports
Member Port(s)	All member ports

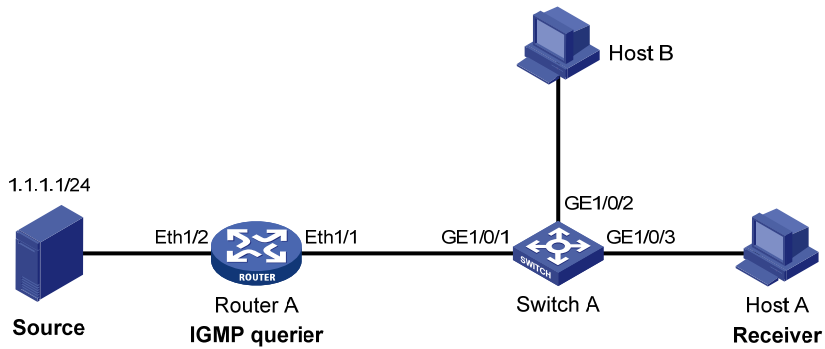
Return to [Configuration task list](#).

IGMP snooping configuration example

Network requirements

- As shown in [a](#), Router A connects to a multicast source (Source) through Ethernet 1/2, and to Switch A through Ethernet 1/1.
- The multicast source sends multicast data to group 224.1.1.1. Host A is a receiver of the multicast group.
- IGMPv2 runs on Router A and IGMP snooping version 2 runs on Switch A.
- The function of dropping unknown multicast packets is enabled on Switch A to prevent Switch A from flooding multicast packets in the VLAN if no corresponding Layer 2 forwarding entry exists.
- The fast leave function is enabled for GigabitEthernet 1/0/3 on Switch A to improve bandwidth and resource usage.

a. Network diagram for IGMP snooping configuration



Configuration procedure

Table 65 Configure IP addresses

Configure the IP address for each interface as per [a](#). The detailed configuration steps are omitted.

Table 66 Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on Ethernet 1/1. The detailed configuration steps are omitted.

Table 67 Configure Switch A

Create VLAN 100 and add GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 100.

- Select **Network** → **VLAN** in the navigation tree and click the **Create** tab to enter the configuration page shown in [b](#).

b. Create VLAN 100

Select VLAN	Create	Port Detail	Detail	Modify VLAN	Modify Port	Remove
-------------	--------	-------------	--------	-------------	-------------	--------

Create:

VLAN IDs:	<input type="text" value="100"/>	Example:3, 5-10
		<input type="button" value="Create"/>

ID	Description
1	VLAN 0001

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID	Description
<input type="text"/>	<input type="text"/>
	(1-32 Chars.)
	<input type="button" value="Apply"/>

- Type the VLAN ID 100.
- Click **Apply** to complete the operation.
- Click the **Modify Port** tab to enter the configuration page shown in c.

c. Add a port to the VLAN

Select VLAN Create Port Detail Detail Modify VLAN **Modify Port** Remove

Select Ports

HP V1910-24G-Po...

Select All Select None Not available for selection

Select membership type:

Untagged Tagged Not A Member Link Type PVID

Enter VLAN IDs to which the port is to be assigned:

VLAN IDs: Example: 1,3,5-10

Selected ports:

Untagged Membership
GE1/0/1-GE1/0/3

Apply Cancel

- Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 in the **Select Ports** field.
 - Select the **Untagged** radio button for **Select membership type**.
 - Type the VLAN ID 100.
 - Click **Apply** to complete the operation.
- # Enable IGMP snooping globally.
- Select **Network** → **IGMP snooping** in the navigation tree to enter the basic configuration page as shown in [d](#).

d. Enable IGMP snooping globally

Basic Advanced

IGMP Snooping: Enable Disable

VLAN Configuration

Search Item: Keywords:

VLAN ID	IGMP Snooping	Version	Drop Unknown	Querier	Query Interval (Sec)	GeneralQuery SourceIP	SpecialQuery SourceIP	Operation
1	Disabled	2	Disabled	Disabled	60	0.0.0.0	0.0.0.0	
100	Disabled	2	Disabled	Disabled	60	0.0.0.0	0.0.0.0	
999	Enabled	2	Disabled	Disabled	60	1.1.1.1	1.1.1.2	

+ Show Entries

- Select **Enable** and click **Apply** to globally enable IGMP snooping.

In VLAN 100, enable IGMP snooping and the function of dropping unknown multicast data.

- Click the icon corresponding to VLAN 100 to enter its configuration page and perform the following configurations, as shown in e.

e. Configure IGMP snooping in the VLAN

Basic Advance

VLAN Configuration

VLAN ID: 100

IGMP Snooping: Enable Disable

Version: 2 3

Drop Unknown: Enable Disable

Querier: Enable Disable

Query Interval: *Seconds (2-300, Default = 60)

General Query Source IP: *IP Address (Default = 0.0.0.0)

Special Query Source IP: *IP Address (Default = 0.0.0.0)

Items marked with an asterisk(*) are required

- Select the **Enable** radio button for **IGMP snooping** and **2** for **Version**.
- Select the **Enable** radio button for **Drop Unknown**.
- Select the **Disable** radio button for **Querier**.

- Click **Apply** to complete the operation.
- # Enable the fast leave function for GigabitEthernet 1/0/3.
- Click the **Advanced** tab.
- f. Configure IGMP snooping on GigabitEthernet 1/0/3**

Basic
Advanced

Port Configuration

Port: GigabitEthernet1/0/3

VLAN ID: 100 *(1-4094 example: 3,5-10) Up to 10 VLAN ranges can be specified.

Multicast Group Limit: (1-255)

Fast Leave: Enable Disable

Items marked with an asterisk(*) are required

Apply

▶ Search Item: VLAN ID Keywords: Search

VLAN ID	Multicast Group Limit	Fast Leave	Operation

- Select GigabitEthernet 1/0/3 from the **Port** drop-down list.
- Type the VLAN ID 100.
- Select the **Enable** radio button for **Fast Leave**.
- Click **Apply** to complete the operation.

Configuration verification

- # Display the IGMP snooping multicast entry information on Switch A.
- Select **Network** → **IGMP Snooping** in the navigation tree to enter the basic configuration page.
 - Click the plus sign (+) in front of **Show Entries** in the basic VLAN configuration page to display information about IGMP snooping multicast entries, as shown in [a](#).

a. IGMP snooping multicast entry information displaying page

— Show Entries

▶ Search Item: VLAN ID Keywords: Search

VLAN ID	Source	Group	Operation
100	0.0.0.0	224.1.1.1	

- Click the icon corresponding to the multicast entry (0.0.0.0, 224.1.1.1) to view information about this entry, as shown in [b](#).

b. Details about an IGMP snooping multicast entry

Entry Details	
VLAN ID:	100
Source Address:	0.0.0.0
Group Address:	224.1.1.1
Router Port(s):	GigabitEthernet1/0/1
Member Port(s):	GigabitEthernet1/0/3

[Back](#)

As shown above, GigabitEthernet 1/0/3 of Switch A is listening to multicast streams destined for multicast group 224.1.1.1.

Routing configuration

NOTE:

The term *router* in this document refers to a switch supporting routing function.

Upon receiving a packet, a router determines the optimal route based on the destination address and forwards the packet to the next router in the path. When the packet reaches the last router, it then forwards the packet to the destination host.

Routing table

Routers forward packets through a routing table. Each entry in the table specifies a physical interface that packets destined for a certain address should go out to reach the next hop—the next router—or the directly connected destination.

Routes in a routing table fall into three categories by origin:

- Direct routes—Routes discovered by data link protocols, also known as “interface routes”.
- Static routes—Routes that are manually configured.
- Dynamic routes—Routes that are discovered dynamically by routing protocols.

A route entry has the following key items:

- Destination IP address—Destination IP address or destination network.
- Mask—Specifies, together with the destination address, the address of the destination network.
- Outbound interface—Specifies the interface through which a matching IP packet is to be forwarded.
- Next hop—Specifies the address of the next hop router on the path.
- Preference of the route—Routes to the same destination can be found by various routing protocols or manually configured; routing protocols and static routes are assigned different preferences. The route with the highest preference (the smallest value) is selected as the optimal route.

Static route

Static routes are manually configured. If a network’s topology is simple, you only need to configure static routes for the network to work properly. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the routes will be unreachable. The network administrator has to modify the static routes manually.

While configuring a static route, specify either the output interface or the next hop address as needed. The next hop address cannot be a local interface IP address; otherwise, the route configuration will not take effect.

It is necessary to identify next hop addresses for all route entries because the router needs to use the next hop address of a matching entry to resolve the corresponding link layer address.

Default route

A default route is used to forward packets that match no entry in the routing table. Without a default route, the packet is discarded.

An IPv4 static default route has both its destination IP address and mask being 0.0.0.0.

Configuring IPv4 routing

Displaying the IPv4 active route table

Select **Network** → **IPv4 Routing** from the navigation tree to enter the page shown in [a](#).

a. Active route table

Summary	Create	Remove
---------	--------	--------

Active route table

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface
127.0.0.0	255.0.0.0	Direct	0	127.0.0.1	InLoopBack0
127.0.0.1	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0
192.168.1.0	255.255.255.0	Direct	0	192.168.1.60	Vlan-interface999
192.168.1.60	255.255.255.255	Direct	0	127.0.0.1	InLoopBack0

2. Description of the fields of the active route table

Field	Description
Destination IP Address	Destination IP address of the route
Mask	Mask of the destination IP address
Protocol	Protocol that discovered the route
Preference	Preference value for the route The smaller the number, the higher the preference.
Next Hop	Next hop IP address of the route
Interface	Output interface of the route. Packets destined for the destination IP address will be forwarded out the interface.

Creating an IPv4 static route

Select **Network** → **IPv4 Routing** from the navigation tree and click the **Create** tab to enter the IPv4 static route configuration page, as shown in [a](#).

a. Create an IPv4 static route

Summary	Create	Remove	
Destination IP Address	<input type="text"/>		
Mask	24 (255.255.255.0) <input type="button" value="v"/>	<input type="checkbox"/> Preference	<input type="text"/> (1-255,Default=60)
Next Hop	<input type="text"/>	<input type="checkbox"/> Interface	NULL0 <input type="button" value="v"/>
<input type="button" value="Apply"/>			

Configured static route information

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface

2. IPv4 static route configuration items

Item	Description
Destination IP Address	Type the destination IP address of the static route, in dotted decimal notation.
Mask	Specify the mask of the destination IP address. Select a mask length (number of consecutive 1s in the mask) or a mask in dotted decimal notation from the drop-down list.
Preference	Type a preference value for the static route. The smaller the number, the higher the preference. For example, specifying the same preference for multiple static routes to the same destination enables load sharing on the routes; specifying different preferences enables route backup.
Next Hop	Type the next hop IP address, in dotted decimal notation.

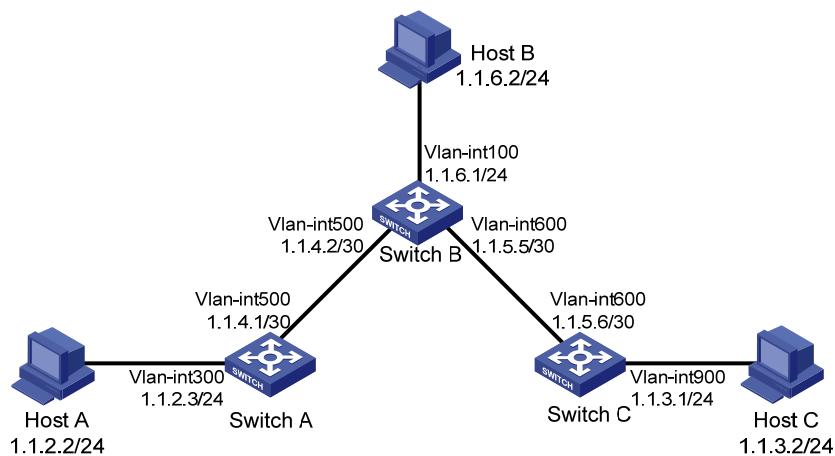
Item	Description
Interface	Select the output interface. You can select any available interface, for example, a virtual interface, of the device. If you select NULL 0 , the destination IP address is unreachable.

Static route configuration example

Network requirements

The IP addresses of devices are shown in a. Configure IPv4 static routes on Switch A, Switch B, and Switch C so that any two hosts can communicate with each other.

a. Network diagram for IPv4 static route configuration



Configuration outlines

Table 68 On Switch A, configure a default route with Switch B as the next hop.

Table 69 On Switch B, configure one static route with Switch A as the next hop and the other with Switch C as the next hop.

Table 70 On Switch C, configure a default route with Switch B as the next hop.

Configuration procedure

Table 71 Configure the IP addresses of the interfaces (omitted)

Table 72 Configure IPv4 static routes

Configure a default route to Switch B on Switch A.

- Select **Network** → **IPv4 Routing** from the navigation tree of Switch A, and then click the **Create** tab to enter the page shown in b.
- Type **0.0.0.0** for **Destination IP Address**.
- Select **0 (0.0.0.0)** from the **Mask** drop-down list.
- Type **1.1.4.2** for **Next Hop**.
- Click **Apply**.

b. Configure a default route

Summary	Create	Remove	
Destination IP Address	0.0.0.0		
Mask	0 (0.0.0.0)	<input type="checkbox"/> Preference	<input type="text"/> (1-255,Default=60)
Next Hop	1.1.4.2	<input type="checkbox"/> Interface	NULL0
<input type="button" value="Apply"/>			

Configured static route information

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface
------------------------	------	----------	------------	----------	-----------

Configure a static route to Switch A and Switch C respectively on Switch B.

- Select **Network** → **IPv4 Routing** from the navigation tree of Switch B, and then click the **Create** tab to enter the page shown in c.
- Type **1.1.2.0** for **Destination IP Address**.
- Select **24 (255.255.255.0)** from the **Mask** drop-down list.
- Type **1.1.4.1** for **Next Hop**.
- Click **Apply**.
- Type **1.1.3.0** for **Destination IP Address**.
- Select **24 (255.255.255.0)** from the **Mask** drop-down list.
- Type **1.1.5.6** for **Next Hop**.
- Click **Apply**.

c. Configure a static route

Summary **Create** Remove

Destination IP Address: 1.1.3.0

Mask: 24 (255.255.255.0)

Next Hop: 1.1.5.6

Preference: (1-255,Default=60)

Interface:

Configured static route information

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface
1.1.2.0	255.255.255.0	Static	60	1.1.4.1	

Configure a default route to Switch B on Switch C.

- Select **Network** → **IPv4 Routing** from the navigation tree of Switch C, and then click the **Create** tab to enter the page as shown in d.
- Type **0.0.0.0** for **Destination IP Address**.
- Select **0 (0.0.0.0)** from the **Mask** drop-down list.
- Type **1.1.5.5** for **Next Hop**.
- Click **Apply**.

d. Configure a default route

Summary	Create	Remove	
Destination IP Address	<input type="text" value="0.0.0.0"/>		
Mask	<input type="text" value="0 (0.0.0.0)"/> ▼	<input type="checkbox"/> Preference	<input type="text" value=""/> (1-255,Default=60)
Next Hop	<input type="text" value="1.1.5.5"/>	<input type="checkbox"/> Interface	<input type="text" value="NULL0"/> ▼
<input type="button" value="Apply"/>			

Configured static route information

Destination IP Address	Mask	Protocol	Preference	Next Hop	Interface

Configuration verification

Display the active route table.

Enter the IPv4 route page of Switch A, Switch B, and Switch C respectively to verify that the newly configured static routes are displayed in the active route table.

Ping Host B from Host A (assuming both hosts run Windows XP).

```
C:\Documents and Settings\Administrator>ping 1.1.3.2
```

```
Pinging 1.1.3.2 with 32 bytes of data:
```

```
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
```

```
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
```

```
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
```

```
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
```

```
Ping statistics for 1.1.3.2:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Precautions

When configuring a static route, note the following:

Table 73 If you do not specify the preference when configuring a static route, the default preference will be used. Reconfiguration of the default preference applies only to newly created static routes. The web interface does not support configuration of the default preference.

Table 74 The static route does not take effect if you specify the next hop address first and then configure it as the IP address of a local interface, such as a VLAN interface.

Table 75 If Null 0 interface is specified as the output interface, the next hop address is not required. If you want to specify a broadcast interface (such as a VLAN interface) as the output interface, which may have multiple next hops, specify the next hop at the same time.

Table 76 You can delete only static routes on the **Remove** tab.

DHCP overview

NOTE:

After the DHCP client is enabled on an interface, the interface can dynamically obtain an IP address and other configuration parameters from the DHCP server. This facilitates configuration and centralized management. For more information about the DHCP client configuration, see the chapter “VLAN interface configuration”.

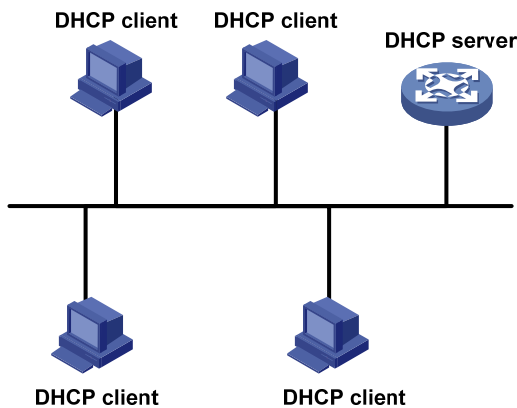
Introduction to DHCP

The fast expansion and growing complexity of networks result in scarce IP addresses assignable to hosts. Meanwhile, as many people need to take their laptops across networks, the IP addresses need to be changed accordingly. Therefore, related configurations on hosts become more complex. The Dynamic Host Configuration Protocol (DHCP) was introduced to solve these problems.

DHCP is built on a client-server model, in which a client sends a configuration request and then the server returns a reply to send configuration parameters such as an IP address to the client.

A typical DHCP application, as shown in a, includes a DHCP server and multiple clients (PCs and laptops).

a. A typical DHCP application



A DHCP client can get an IP address and other configuration parameters from a DHCP server on another subnet via a DHCP relay agent. For more information about the DHCP relay agent configuration, see the chapter “DHCP relay agent configuration”.

DHCP address allocation

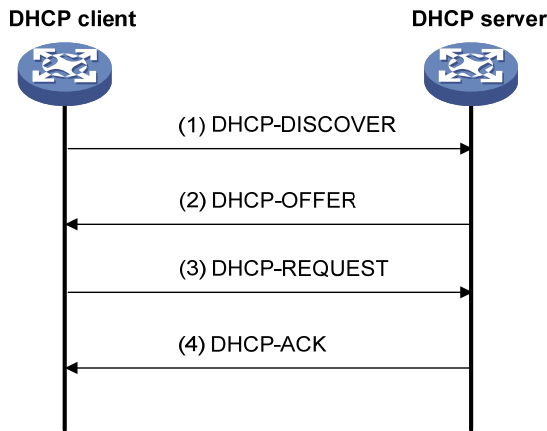
Allocation mechanisms

DHCP supports three mechanisms for IP address allocation.

- Manual allocation: The network administrator assigns an IP address to a client like a WWW server, and DHCP conveys the assigned address to the client.
- Automatic allocation: DHCP assigns a permanent IP address to a client.
- Dynamic allocation: DHCP assigns an IP address to a client for a limited period of time, which is called a lease. Most DHCP clients obtain their addresses in this way.

Dynamic IP address allocation process

a. Dynamic IP address allocation process



As shown in a, a DHCP client obtains an IP address from a DHCP server via four steps:

Table 77 The client broadcasts a DHCP-DISCOVER message to locate a DHCP server.

Table 78 A DHCP server offers configuration parameters such as an IP address to the client in a DHCP-OFFER message. The sending mode of the DHCP-OFFER is determined by the flag field in the DHCP-DISCOVER message.

Table 79 If several DHCP servers send offers to the client, the client accepts the first received offer, and broadcasts it in a DHCP-REQUEST message to request the IP address formally.

Table 80 All DHCP servers receive the DHCP-REQUEST message, but only the server from which the client accepts the offered IP address returns a DHCP-ACK message to the client, confirming that the IP address has been allocated to the client, or a DHCP-NAK unicast message, denying the IP address allocation.

NOTE:

After the client receives the DHCP-ACK message, it will probe whether the IP address assigned by the server is in use by broadcasting a gratuitous ARP packet. If the client receives no response within the specified time, the client can use this IP address. Otherwise, the client sends a DHCP-DECLINE message to the server and requests an IP address again.

IP addresses offered by other DHCP servers are still assignable to other clients.

IP address lease extension

The IP address dynamically allocated by a DHCP server to a client has a lease. When the lease expires, the DHCP server will reclaim the IP address. If the client wants to use the IP address longer, it has to extend the lease duration.

When the half lease duration elapses, the DHCP client sends to the DHCP server a DHCP-REQUEST unicast to extend the lease duration. Upon availability of the IP address, the DHCP server returns a DHCP-ACK unicast confirming that the client's lease duration has been extended, or a DHCP-NAK unicast denying the request.

If the client receives no reply, it will broadcast another DHCP-REQUEST message for lease extension after 7/8 lease duration elapses. The DHCP server will handle the request as above mentioned.

DHCP message format

α gives the DHCP message format, which is based on the BOOTP message format and involves eight types. These types of messages have the same format except that some fields have different values. The numbers in parentheses indicate the size of each field in bytes.

α. DHCP message format

0	7	15	23	31
op (1)		htype (1)		hlen (1)
xid (4)				
secs (2)			flags (2)	
ciaddr (4)				
yiaddr (4)				
siaddr (4)				
giaddr (4)				
chaddr (16)				
sname (64)				
file (128)				
options (variable)				

- op: Message type defined in option field. 1 = REQUEST, 2 = REPLY
- htype, hlen: Hardware address type and length of a DHCP client.
- hops: Number of relay agents a request message traveled.
- xid: Transaction ID, a random number chosen by the client to identify an IP address allocation.
- secs: Filled in by the client, the number of seconds elapsed since the client began address acquisition or renewal process. This field is reserved and set to 0.
- flags: The leftmost bit is defined as the BROADCAST (B) flag. If this flag is set to 0, the DHCP server sent a reply back by unicast; if this flag is set to 1, the DHCP server sent a reply back by broadcast. The remaining bits of the flags field are reserved for future use.
- ciaddr: Client IP address.
- yiaddr: 'your' (client) IP address, assigned by the server.
- siaddr: Server IP address, from which the clients obtained configuration parameters.
- giaddr: IP address of the first relay agent a request message traveled.
- chaddr: Client hardware address.
- sname: Server host name, from which the client obtained configuration parameters.

- file: Bootfile name and path information, defined by the server to the client.
- options: Optional parameters field that is variable in length, which includes the message type, lease, domain name server IP address, and WINS IP address.

DHCP options

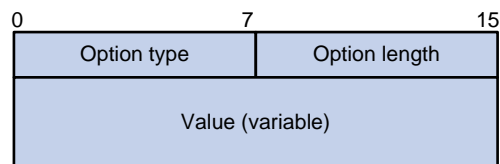
DHCP options overview

The DHCP message adopts the same format as the Bootstrap Protocol (BOOTP) message for compatibility, but differs from it in the option field, which identifies new features for DHCP.

DHCP uses the option field in DHCP messages to carry control information and network configuration parameters, implementing dynamic address allocation and providing more network configuration information for clients.

a shows the DHCP option format.

a. DHCP option format



Introduction to DHCP options

The common DHCP options are as follows:

- Option 6: DNS server option. It specifies the DNS server IP address to be assigned to the client.
- Option 51: IP address lease option.
- Option 53: DHCP message type option. It identifies the type of the DHCP message.
- Option 55: Parameter request list option. It is used by a DHCP client to request specified configuration parameters. The option contains values that correspond to the parameters requested by the client.
- Option 66: TFTP server name option. It specifies a TFTP server to be assigned to the client.
- Option 67: Bootfile name option. It specifies the bootfile name to be assigned to the client.
- Option 150: TFTP server IP address option. It specifies the TFTP server IP address to be assigned to the client.
- Option 121: Classless route option. It specifies a list of classless static routes (the destination addresses in these static routes are classless) that the requesting client should add to its routing table.
- Option 33: Static route option. It specifies a list of classful static routes (the destination addresses in these static routes are classful) that a client should add to its routing table. If Option 121 exists, Option 33 is ignored.

For more information about DHCP options, see RFC 2132.

Introduction to Option 82

Some options, such as Option 82, have no unified definitions in RFC 2132.

Option 82 is the relay agent option in the option field of the DHCP message. It records the location information of the DHCP client. When a DHCP relay agent or DHCP snooping device receives a client's request, it adds Option 82 to the request message before forwarding the message to the server.

The administrator can locate the DHCP client to further implement security control and accounting. The Option 82 supporting server can also use such information to define individual assignment policies of IP address and other parameters for the clients.

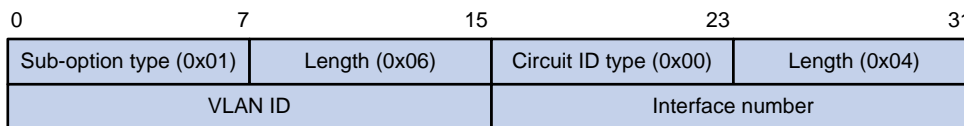
Option 82 involves at most 255 sub-options. At least one sub-option is defined. The DHCP relay agent supports two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID).

Option 82 has no unified definition. Its padding formats vary with vendors.

By default, the normal padding format is used on the device. You can specify the code type for the sub-options as ASCII or HEX. The padding contents for sub-options in the normal padding format are as follows:

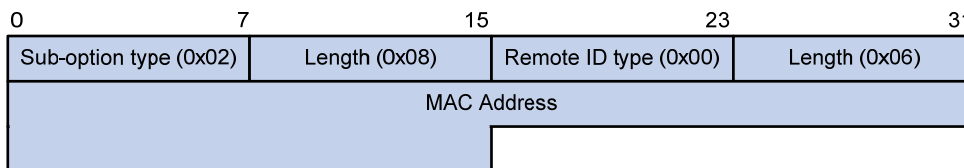
- Sub-option 1: Padded with the VLAN ID and interface number of the interface that received the client's request. a gives its format. The value of the sub-option type is 1, and that of the circuit ID type is 0.

a. Sub-option 1 in normal padding format



- Sub-option 2: Padded with the MAC address of the DHCP relay agent interface or the MAC address of the DHCP snooping device that received the client's request. b gives its format. The value of the sub-option type is 2, and that of the remote ID type is 0.

b. Sub-option 2 in normal padding format



Protocols and standards

- RFC 2131, *Dynamic Host Configuration Protocol*
- RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
- RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
- RFC 3046, *DHCP Relay Agent Information Option*

DHCP relay agent configuration

Introduction to DHCP relay agent

Application environment

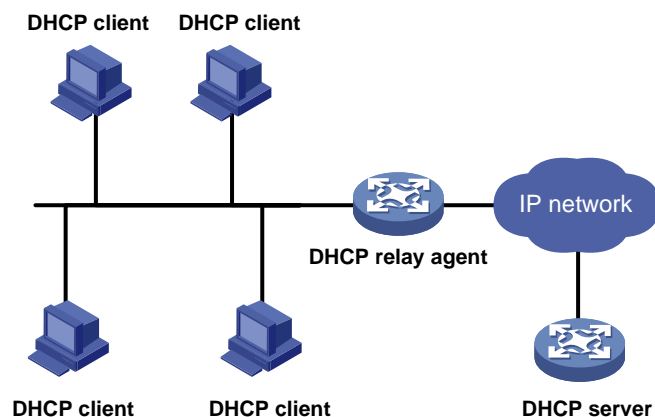
Since DHCP clients request IP addresses via broadcast messages, the DHCP server and clients must be on the same subnet. Therefore, a DHCP server must be available on each subnet, which is not practical.

DHCP relay agent solves the problem. Via a relay agent, DHCP clients communicate with a DHCP server on another subnet to obtain configuration parameters. Thus, DHCP clients on different subnets can contact the same DHCP server, and centralized management and cost reduction are achieved.

Fundamentals

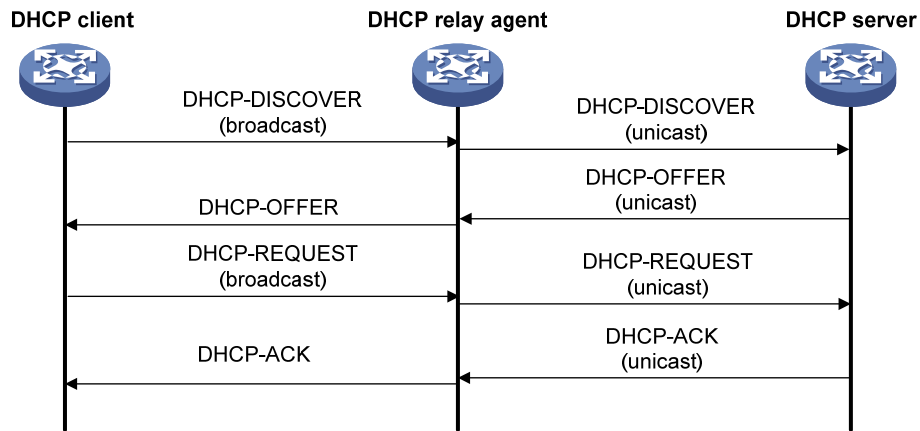
a shows a typical application of the DHCP relay agent.

a. DHCP relay agent application



No matter whether a relay agent exists or not, the DHCP server and client interact with each other in a similar way (see the chapter "[DHCP overview](#)"). The following describes the forwarding process on the DHCP relay agent.

b. DHCP relay agent work process



As shown in [b](#), the DHCP relay agent works as follows:

Table 81 After receiving a DHCP-DISCOVER or DHCP-REQUEST broadcast message from a DHCP client, the DHCP relay agent fills the giaddr field of the message with its IP address and forwards the message to the designated DHCP server in unicast mode.

Table 82 Based on the giaddr field, the DHCP server returns an IP address and other configuration parameters to the relay agent, which conveys them to the client.

DHCP relay agent configuration task list

Complete the following tasks to configure the DHCP relay agent:

Task	Remarks
Enabling DHCP and configuring advanced parameters for the DHCP relay agent	<p>Required</p> <p>Enable DHCP globally and configure advanced DHCP parameters. By default, global DHCP is disabled.</p>
Creating a DHCP server group	<p>Required</p> <p>To improve reliability, you can specify several DHCP servers as a group on the DHCP relay agent and correlate a relay agent interface with the server group. When the interface receives requesting messages from clients, the relay agent will forward them to all the DHCP servers of the group.</p>
Enabling the DHCP relay agent on an interface	<p>Required</p> <p>Enable the DHCP relay agent on an interface, and correlate the interface with a DHCP server group.</p> <p>With DHCP enabled, interfaces work in the DHCP server mode by default.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> You can enable either the DHCP server or the DHCP relay agent on an interface. The latest configuration takes effect. The DHCP relay agent works on interfaces with IP addresses manually configured only.

Task	Remarks
Configuring and displaying clients' IP-to-MAC bindings	<p>Optional</p> <p>Create a static IP-to-MAC binding, and view static and dynamic bindings.</p> <p>The DHCP relay agent can dynamically record clients' IP-to-MAC bindings after clients get IP addresses. It also supports static bindings, that is, you can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external network using fixed IP addresses.</p> <p>By default, no static binding is created.</p>

Enabling DHCP and configuring advanced parameters for the DHCP relay agent

Select **Network** → **DHCP** from the navigation tree to enter the default **DHCP Relay** page. Enable or disable DHCP in the **DHCP Service** field. Click **Display Advanced Configuration** to expand the advanced DHCP relay agent configuration field, as shown in [a](#).

a. DHCP relay agent configuration page

DHCP Relay

DHCP Snooping

DHCP Service Enable Disable

Hide Advanced Configuration

Unauthorized Server Detect Enable Disable

Dynamic Bindings Refresh Enable Disable

Track Timer Interval Auto Custom Seconds (1-120)

Server Group

▶ Search Item: Server Group ID Keywords:

Server Group ID	IP Address	Operation
<input type="button" value="Add"/>		

Interface Config

▶ Search Item: Interface Name Keywords:

Interface Name	DHCP Relay State	Operation
Vlan-interface1	Enabled	<input type="button" value="ⓘ"/>

User Information

User Information

2. DHCP service and advanced DHCP relay agent configuration items

Item	Description
DHCP Service	Enable or disable global DHCP.
Unauthorized Server Detect	<p>Enable or disable unauthorized DHCP server detection.</p> <p>There are unauthorized DHCP servers on networks, which reply DHCP clients with wrong IP addresses.</p> <p>With this feature enabled, upon receiving a DHCP request, the DHCP relay agent will record the IP address of any DHCP server that assigned an IP address to the DHCP client and the receiving interface. The administrator can use this information to check out DHCP unauthorized servers. The device puts a record once for each DHCP server. The administrator needs to find unauthorized DHCP servers from the log information. After the information of recorded DHCP servers is cleared, the relay agent will re-record server information following this mechanism.</p>
Dynamic Bindings Refresh	<p>Enable or disable periodic refresh of dynamic client entries, and set the refresh interval.</p> <p>Via the DHCP relay agent, a DHCP client sends a DHCP-RELEASE unicast message to the DHCP server to relinquish its IP address. In this case the DHCP relay agent simply conveys the message to the DHCP server, thus it does not remove the IP address from dynamic client entries. To solve this problem, the periodic refresh of dynamic client entries feature is introduced.</p> <p>With this feature, the DHCP relay agent uses the IP address of a client and the MAC address of the DHCP relay agent interface to periodically send a DHCP-REQUEST message to the DHCP server.</p>
Track Timer Interval	<ul style="list-style-type: none">• If the server returns a DHCP-ACK message or does not return any message within a specified interval, which means that the IP address is assignable now, the DHCP relay agent will age out the client entry.• If the server returns a DHCP-NAK message, which means the IP address is still in use, the relay agent will not age it out. <p>Note that if the Auto radio button is clicked on, the refresh interval is calculated by the relay agent according to the number of client entries.</p>

Return to [DHCP relay agent configuration task list](#).

Creating a DHCP server group

Select **Network** → **DHCP** from the navigation tree to enter the default **DHCP Relay** page shown in [a](#). In the **Server Group** field, click **Add** to enter the page shown in [a](#).

a. Create a server group


DHCP Relay	DHCP Snooping	
Server Group ID	<input type="text"/>	*(0-19)
IP Address	<input type="text"/>	*
Items marked with an asterisk(*) are required		
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

2. DHCP server group configuration items

Item	Description
Server Group ID	Type the ID of a DHCP server group. You can create up to 20 DHCP server groups.
IP Address	Type the IP address of a server in the DHCP server group. The server IP address cannot be on the same subnet as the IP address of the DHCP relay agent; otherwise, the client cannot obtain an IP address.

Return to [DHCP relay agent configuration task list](#).

Enabling the DHCP relay agent on an interface

Select **Network** → **DHCP** from the navigation tree to enter the default **DHCP Relay** page shown in [a](#). In the **Interface Config** field, the DHCP relay agent state of interfaces is displayed. Click the  icon of a specific interface to enter the page shown in [a](#).

a. Configure a DHCP relay agent interface

DHCP Relay	DHCP Snooping	
Interface Name	Vlan-interface1	
DHCP Relay	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Address Match Check	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Server Group ID	<input type="text"/> *	

Items marked with an asterisk(*) are required

2. DHCP relay agent interface configuration items

Item	Description
Interface Name	This field displays the name of a specific interface.
DHCP Relay	Enable or disable the DHCP relay agent on the interface.
Address Match Check	Enable or disable IP address check. With this function enabled, the DHCP relay agent checks whether a requesting client's IP and MAC addresses match a binding (dynamic or static) on the DHCP relay agent. If not, the client cannot access outside networks via the DHCP relay agent. This prevents invalid IP address configuration.
Server Group ID	Correlate the interface with a DHCP server group. A DHCP server group can be correlated with multiple interfaces.

Return to [DHCP relay agent configuration task list](#).

Configuring and displaying clients' IP-to-MAC bindings

Select **Network** → **DHCP** from the navigation tree to enter the default **DHCP Relay** page shown in a. In the **User Information** field, click the **User Information** button to view static and dynamic bindings, as shown in a. Click **Add** to enter the page shown in b.

a. Display clients' IP-to-MAC bindings

DHCP Relay | DHCP Snooping

▶ Search Item: IP Address | Keywords: | Search

IP Address	MAC Address	Type	Interface Name	Operation
1.1.1.10	00e0-1234-5678	Static	Vlan-interface1	

Add | Return | Refresh | Reset

b. Create a static IP-to-MAC binding

DHCP Relay | DHCP Snooping

IP Address *

MAC Address *(H-H-H)

Interface Name

Items marked with an asterisk(*) are required

Apply | Cancel

2. Static IP-to-MAC binding configuration items

Item	Description
IP Address	Type the IP address of a DHCP client.
MAC Address	Type the MAC address of the DHCP client.
Interface Name	Select the Layer 3 interface connected with the DHCP client. IMPORTANT: The interface of a static binding entry must be configured as a DHCP relay agent; otherwise, address entry conflicts may occur.

Return to [DHCP relay agent configuration task list](#).

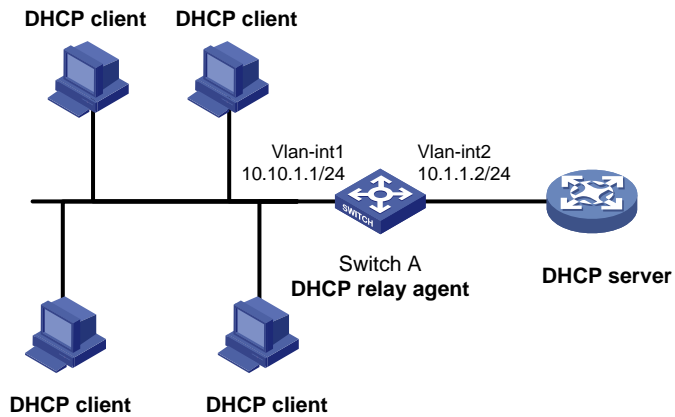
DHCP relay agent configuration example

Network requirements

As shown in a, VLAN-interface 1 on the DHCP relay agent (Switch A) connects to the network where DHCP clients reside. The IP address of VLAN-interface 1 is 10.10.1.1/24 and the IP address of VLAN-interface 2 is 10.1.1.1/24. VLAN-interface 2 is connected to the DHCP server whose IP address is 10.1.1.1/24.

The switch forwards messages between DHCP clients and the DHCP server.

a. Network diagram for DHCP relay agent configuration



Configuration procedure

Table 83 Specify IP addresses for interfaces (omitted)

Table 84 Configure the DHCP relay agent

Enable DHCP.

- Select **Network** → **DHCP** from the navigation tree to enter the default **DHCP Relay** page. Perform the following operations, as shown in b.

b. Enable DHCP

DHCP Relay | DHCP Snooping

DHCP Service Enable Disable

Display Advanced Configuration

Apply Cancel

Server Group

Search Item: Server Group ID Keywords: Search

Server Group ID	IP Address	Operation
Add		

Interface Config

Search Item: Interface Name Keywords: Search

Interface Name	DHCP Relay State	Operation
Vlan-interface1	Disabled	
Vlan-interface2	Disabled	

User Information

User Information

- Click on the **Enable** radio button next to **DHCP Service**.
- Click **Apply**.

Configure a DHCP server group.

- In the **Server Group** field, click **Add** and then perform the following operations, as shown in c.

c. Add a DHCP server group

DHCP Relay | DHCP Snooping


Server Group ID *(0-19)

IP Address *

Items marked with an asterisk(*) are required

Apply Cancel

- Type **1** for **Server Group ID**.
- Type **10.1.1.1** for **IP Address**.

- Click **Apply**.
- # Enable the DHCP relay agent on VLAN-interface 1.
- In the **Interface Config** field, click the  icon of VLAN-interface 1, and then perform the following operations, as shown in d.
- d. **Enable the DHCP relay agent on an interface and correlate it with a server group**

DHCP Relay	DHCP Snooping	
Interface Name	Vlan-interface1	
DHCP Relay	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Address Match Check	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Server Group ID	1 *	

Items marked with an asterisk(*) are required

- Click on the **Enable** radio button next to **DHCP Relay**.
- Select **1** for **Server Group ID**.
- Click **Apply**.

NOTE:

Because the DHCP relay agent and server are on different subnets, you need to configure a static route or dynamic routing protocol to make them reachable to each other.

DHCP snooping configuration

NOTE:

A DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.

HP recommends you not to enable the DHCP client, BOOTP client, and DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client/DHCP client may fail to obtain an IP address.

DHCP snooping overview

Functions of DHCP snooping

As a DHCP security feature, DHCP snooping can implement the following:

Table 85 Recording IP-to-MAC mappings of DHCP clients

Table 86 Ensuring DHCP clients to obtain IP addresses from authorized DHCP servers

Recording IP-to-MAC mappings of DHCP clients

DHCP snooping reads DHCP-REQUEST messages and DHCP-ACK messages from trusted ports to record DHCP snooping entries, including MAC addresses of clients, IP addresses obtained by the clients, ports that connect to DHCP clients, and VLANs to which the ports belong.

Ensuring DHCP clients to obtain IP addresses from authorized DHCP servers

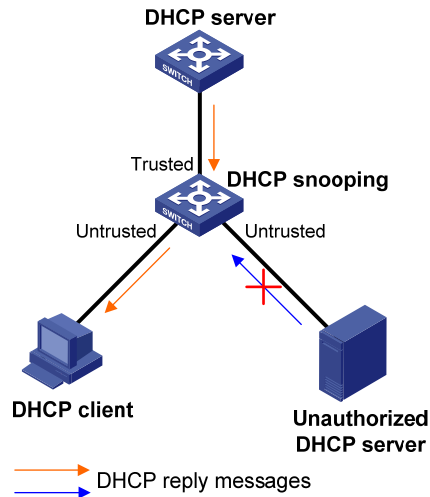
If there is an unauthorized DHCP server on a network, DHCP clients may obtain invalid IP addresses and network configuration parameters, and cannot normally communicate with other network devices. With DHCP snooping, the ports of a device can be configured as trusted or untrusted, ensuring the clients to obtain IP addresses from authorized DHCP servers.

- Trusted: A trusted port forwards DHCP messages normally.
- Untrusted: An untrusted port discards the DHCP-ACK or DHCP-OFFER messages received from any DHCP server.

Application environment of trusted ports

Configuring a trusted port connected to a DHCP server

a. Configure trusted and untrusted ports



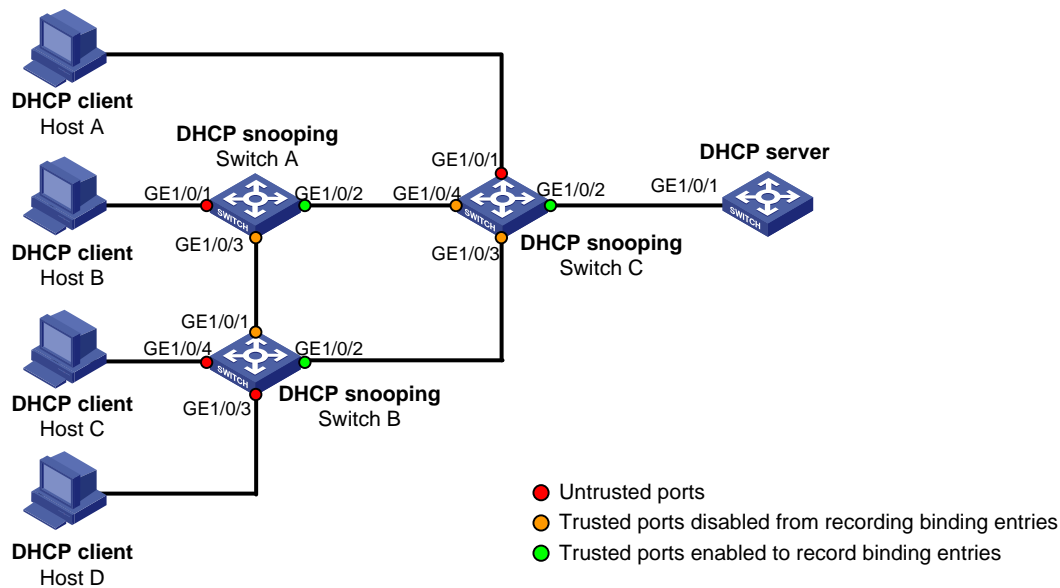
As shown in a, a DHCP snooping device's port that is connected to an authorized DHCP server should be configured as a trusted port to forward reply messages from the DHCP server, so that the DHCP client can obtain an IP address from the authorized DHCP server.

Configuring trusted ports in a cascaded network

In a cascaded network involving multiple DHCP snooping devices, the ports connected to other DHCP snooping devices should be configured as trusted ports.

To save system resources, you can disable the trusted ports, which are indirectly connected to DHCP clients, from recording clients' IP-to-MAC bindings upon receiving DHCP requests.

a. Configure trusted ports in a cascaded network



2 describes roles of the ports shown in a.

2. Roles of ports

Device	Untrusted port	Trusted port disabled from recording binding entries	Trusted port enabled to record binding entries
Switch A	GigabitEthernet 1/0/1	GigabitEthernet 1/0/3	GigabitEthernet 1/0/2
Switch B	GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4	GigabitEthernet 1/0/1	GigabitEthernet 1/0/2
Switch C	GigabitEthernet 1/0/1	GigabitEthernet 1/0/3 and GigabitEthernet 1/0/4	GigabitEthernet 1/0/2

DHCP snooping support for Option 82

Option 82 records the location information of the DHCP client. The administrator can locate the DHCP client to further implement security control and accounting. For more information, see the chapter “DHCP overview”.

If DHCP snooping supports Option 82, it will handle a client’s request according to the contents defined in Option 82, if any. The handling strategies are described in the table below.

If a reply returned by the DHCP server contains Option 82, the DHCP snooping device will remove the Option 82 before forwarding the reply to the client. If the reply contains no Option 82, the DHCP snooping device forwards it directly.

If a client’s requesting message has...	Handling strategy	The DHCP snooping device will...
Option 82	Drop	Drop the message.
	Keep	Forward the message without changing Option 82.
	Replace	Forward the message after replacing the original Option 82 with the Option 82 padded in normal format.
no Option 82	—	Forward the message after adding the Option 82 padded in normal format.

DHCP snooping configuration task list

Complete the following tasks to configure DHCP snooping:

Task	Remarks
Enabling DHCP snooping	Required By default, DHCP snooping is disabled.

Task	Remarks
Configuring DHCP snooping functions on an interface	<p>Required</p> <p>Specify an interface as trusted and configure DHCP snooping to support Option 82.</p> <p>By default, an interface is untrusted and DHCP snooping does not support Option 82.</p> <p>! IMPORTANT:</p> <p>You need to specify the ports connected to the authorized DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses. The trusted port and the port connected to the DHCP client must be in the same VLAN.</p>
Displaying clients' IP-to-MAC bindings	<p>Optional</p> <p>Display clients' IP-to-MAC bindings recorded by DHCP snooping.</p>

Enabling DHCP snooping

Select **Network** → **DHCP** from the navigation tree, and then click the **DHCP Snooping** tab to enter the page shown in [a](#). You can enable or disable DHCP snooping in the **DHCP Snooping** field.

a. **DHCP snooping configuration page**

DHCP Relay **DHCP Snooping**

DHCP Snooping

DHCP Snooping Enable Disable

Interface Config

▶ Search Item: **Interface Name** Keywords: Search

Interface Name	Interface State	Operation
GigabitEthernet1/0/1	Untrust	
GigabitEthernet1/0/2	Untrust	
GigabitEthernet1/0/3	Untrust	
GigabitEthernet1/0/4	Untrust	
GigabitEthernet1/0/5	Untrust	
GigabitEthernet1/0/6	Untrust	
GigabitEthernet1/0/7	Untrust	
GigabitEthernet1/0/8	Untrust	
GigabitEthernet1/0/9	Untrust	
GigabitEthernet1/0/10	Untrust	
GigabitEthernet1/0/11	Untrust	
GigabitEthernet1/0/12	Untrust	
GigabitEthernet1/0/13	Untrust	
GigabitEthernet1/0/14	Untrust	
GigabitEthernet1/0/15	Untrust	

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO


User Information

User Information

- To enable DHCP snooping, click on the **Enable** radio button in the **DHCP Snooping** field.
- To disable DHCP snooping, click on the **Disable** radio button in the **DHCP Snooping** field.

Return to [DHCP snooping configuration task list](#).

Configuring DHCP snooping functions on an interface

Select **Network** → **DHCP** from the navigation tree, and then click the **DHCP Snooping** tab to enter the page shown in [a](#). You can view trusted and untrusted ports in the **Interface Config** field. Click the  icon of a specific interface to enter the page shown in [a](#).

a. DHCP snooping interface configuration page



2. DHCP snooping interface configuration items

Item	Description
Interface Name	This field displays the name of a specific interface.
Interface State	Configure the interface as trusted or untrusted.
Option 82 Support	Configure DHCP snooping to support Option 82 or not.
Option 82 Strategy	Select the handling strategy for DHCP requests containing Option 82. The strategies include: <ul style="list-style-type: none">• Drop: The message is discarded if it contains Option 82.• Keep: The message is forwarded without its Option 82 being changed.• Replace: The message is forwarded after its original Option 82 is replaced with the Option 82 padded in normal format.

Return to [DHCP snooping configuration task list](#).

Displaying clients' IP-to-MAC bindings

Select **Network** → **DHCP** from the navigation tree, and then click the **DHCP Snooping** tab to enter the page shown in [a](#). Click the **User Information** button to view clients' IP-to-MAC bindings recorded by DHCP snooping, as shown in [a](#).

a. DHCP snooping user information

DHCP Relay DHCP Snooping

▶ Search Item: IP Address Keywords: Search

IP Address	MAC Address	Type	Interface Name	VLAN	Remaining Lease Time (Sec)	Operation
1.0.0.2	00e0-fc00-5801	Dynamic	GigabitEthernet1/0/1	1	86353	

Return Refresh Reset

2. DHCP snooping user information configuration items

Item	Description
IP Address	This field displays the IP address assigned by the DHCP server to the client.
MAC Address	This field displays the MAC address of the client.
Type	This field displays the client type, which can be: <ul style="list-style-type: none">• Dynamic: The IP-to-MAC binding is generated dynamically.• Static: The IP-to-MAC binding is configured manually. Static bindings are not supported.
Interface Name	This field displays the device interface to which the client is connected.
VLAN	This field displays the VLAN to which the device belongs.
Remaining Lease Time	This field displays the remaining lease time of the IP address.

Return to [DHCP snooping configuration task list](#).

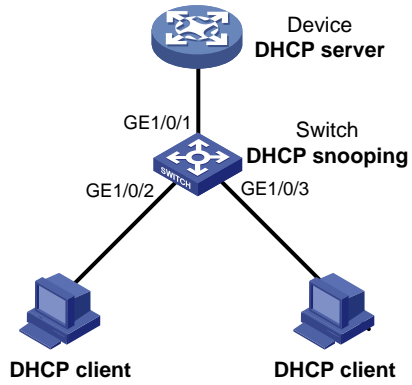
DHCP snooping configuration example

Network requirements

As shown in a, a DHCP snooping device (Switch) is connected to a DHCP server through GigabitEthernet 1/0/1, and to DHCP clients through GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3.

- Enable DHCP snooping on Switch and configure DHCP snooping to support Option 82. Configure the handling strategy for DHCP requests containing Option 82 as **replace**.
- Enable GigabitEthernet 1/0/1 to forward DHCP server responses; disable GigabitEthernet 1/0/2 and GigabitEthernet 1/0/3 from forwarding DHCP server responses.
- Configure Switch to record clients' IP-to-MAC address bindings in DHCP-REQUEST messages and DHCP-ACK messages received from a trusted port.

a. Network diagram for DHCP snooping configuration



Configuration procedure

Enable DHCP snooping.

- Select **Network** → **DHCP** from the navigation tree, and then click the **DHCP Snooping** tab. Perform the following operation, as shown in a.

a. Enable DHCP snooping

DHCP Relay DHCP Snooping

DHCP Snooping Enable Disable

Interface Config

▶ Search Item: Interface Name Keywords: Search

Interface Name	Interface State	Operation
GigabitEthernet1/0/1	Untrust	
GigabitEthernet1/0/2	Untrust	
GigabitEthernet1/0/3	Untrust	
GigabitEthernet1/0/4	Untrust	
GigabitEthernet1/0/5	Untrust	
GigabitEthernet1/0/6	Untrust	
GigabitEthernet1/0/7	Untrust	
GigabitEthernet1/0/8	Untrust	
GigabitEthernet1/0/9	Untrust	
GigabitEthernet1/0/10	Untrust	
GigabitEthernet1/0/11	Untrust	
GigabitEthernet1/0/12	Untrust	
GigabitEthernet1/0/13	Untrust	
GigabitEthernet1/0/14	Untrust	
GigabitEthernet1/0/15	Untrust	

28 records, 15 per page | page 1/2, record 1-15 | First Prev Next Last 1 GO

User Information

User Information


- Click on the **Enable** radio button next to **DHCP Snooping**.
- # Configure DHCP snooping functions on GigabitEthernet 1/0/1.
- Click the icon of GigabitEthernet 1/0/1 on the interface list. Perform the following operations on the **DHCP Snooping Interface Configuration** page shown in b.

b. Configure DHCP snooping functions on GigabitEthernet 1/0/1

DHCP Relay	DHCP Snooping
Interface Name	GigabitEthernet1/0/1
Interface State	<input checked="" type="radio"/> Trust <input type="radio"/> Untrust
Option 82 Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Option 82 Strategy	Replace (Default = Replace)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click on the **Trust** radio button next to **Interface State**.
- Click **Apply**.

Configure DHCP snooping functions on GigabitEthernet 1/0/2.


- Click the  icon of GigabitEthernet 1/0/2 on the interface list. Perform the following operations on the **DHCP Snooping Interface Configuration** page shown in [c](#).

c. Configure DHCP snooping functions on GigabitEthernet 1/0/2

DHCP Relay	DHCP Snooping
Interface Name	GigabitEthernet1/0/2
Interface State	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
Option 82 Support	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Option 82 Strategy	Replace (Default = Replace)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click on the **Untrust** radio button for **Interface State**.
- Click on the **Enable** radio button next to **Option 82 Support**.
- Select **Replace** for **Option 82 Strategy**.
- Click **Apply**.

Configure DHCP snooping functions on GigabitEthernet 1/0/3.

- Click the  icon of GigabitEthernet 1/0/3 on the interface list. Perform the following operations on the **DHCP Snooping Interface Configuration** page shown in [d](#).

d. Configure DHCP snooping functions on GigabitEthernet 1/0/3

DHCP Relay	DHCP Snooping
Interface Name	GigabitEthernet1/0/3
Interface State	<input type="radio"/> Trust <input checked="" type="radio"/> Untrust
Option 82 Support	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Option 82 Strategy	Replace (Default = Replace)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- Click on the **Untrust** radio button for **Interface State**.
- Click on the **Enable** radio button next to **Option 82 Support**.
- Select **Replace** for **Option 82 Strategy**.
- Click **Apply**.

Service management configuration

The service management module provides the following types of services: FTP, Telnet, SSH, SFTP, HTTP and HTTPS. You can enable or disable the services as needed. In this way, the performance and security of the system can be enhanced, thus secure management of the device can be achieved.

The service management module also provides the function to modify HTTP and HTTPS port numbers, and the function to associate the FTP, HTTP, or HTTPS service with an ACL, thus reducing attacks of illegal users on these services.

FTP service

The File Transfer Protocol (FTP) is an application layer protocol for sharing files between server and client over a TCP/IP network.

Telnet service

The Telnet protocol is an application layer protocol that provides remote login and virtual terminal functions on the network.

SSH service

Secure Shell (SSH) offers an approach to securely logging in to a remote device. By encryption and strong authentication, it protects devices against attacks such as IP spoofing and plain text password interception.

SFTP service

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 serve as an SFTP client, enabling a user to login from the device to a remote device for secure file transfer.

HTTP service

The Hypertext Transfer Protocol (HTTP) is used for transferring web page information across the Internet. It is an application-layer protocol in the TCP/IP protocol suite.

You can log in to the device using the HTTP protocol with HTTP service enabled, accessing and controlling the device with Web-based network management.

HTTPS service

The Secure HTTP (HTTPS) refers to the HTTP protocol that supports the Security Socket Layer (SSL) protocol.

The SSL protocol of HTTPS enhances the security of the device in the following ways:

- Uses the SSL protocol to ensure the legal clients to access the device securely and prohibit the illegal clients;
- Encrypts the data exchanged between the HTTPS client and the device to ensure the data security and integrity, thus realizing the security management of the device;
- Defines certificate attribute-based access control policy for the device to control the access right of the client, in order to further avoid attacks from illegal clients.

Configuring service management

Select **Network** → **Service** from the navigation tree to enter the service management configuration page, as shown in a.

a. Service management

Service

Service Management



+FTP	<input type="checkbox"/> Enable FTP service
Telnet	<input checked="" type="checkbox"/> Enable Telnet service
SSH	<input type="checkbox"/> Enable SSH service
SFTP	<input type="checkbox"/> Enable SFTP service
+HTTP	<input checked="" type="checkbox"/> Enable HTTP service
+HTTPS	<input type="checkbox"/> Enable HTTPS service

PKI Domain:

Items marked with an asterisk(*) are required

2. Service management configuration items

Item		Description
FTP	Enable FTP service	Specify whether to enable the FTP service. The FTP service is disabled by default.
	ACL	Associate the FTP service with an ACL. Only the clients that pass the ACL filtering are permitted to use the FTP service. You can view this configuration item by clicking the expanding button in front of FTP .
Telnet	Enable Telnet service	Specify whether to enable the Telnet service. The Telnet service is disabled by default.
SSH	Enable SSH service	Specify whether to enable the SSH service. The SSH service is disabled by default.
SFTP	Enable SFTP service	Specify whether to enable the SFTP service. The SFTP service is disabled by default. ! IMPORTANT: When you enable the SFTP service, the SSH service must be enabled.
HTTP	Enable HTTP service	Specify whether to enable the HTTP service. The HTTP service is enabled by default.

Item	Description
Port Number	<p>Set the port number for HTTP service.</p> <p>You can view this configuration item by clicking the expanding button in front of HTTP.</p> <p> IMPORTANT:</p> <p>When you modify a port, ensure that the port is not used by other service.</p>
	<p>Associate the HTTP service with an ACL. Only the clients that pass the ACL filtering are permitted to use the HTTP service.</p> <p>You can view this configuration item by clicking the expanding button in front of HTTP.</p>
Enable HTTPS service	<p>Specify whether to enable the HTTPS service.</p> <p>The HTTPS service is disabled by default.</p>
HTTPS	<p>Set the port number for HTTPS service.</p> <p>You can view this configuration item by clicking the expanding button in front of HTTPS.</p> <p> IMPORTANT:</p> <p>When you modify a port, ensure that the port is not used by other service.</p>
	<p>Associate the HTTPS service with an ACL. Only the clients that pass the ACL filtering are permitted to use the HTTPS service.</p> <p>You can view this configuration item by clicking the expanding button in front of HTTPS.</p>
	<p>Set the PKI domain for the HTTPS service.</p> <p>You can configure the available PKI domains by selecting Authentication → PKI from the navigation tree at the left side of the interface. For more information, see the chapter “PKI configuration”.</p>

Diagnostic tools

Ping

The **ping** command allows you to verify whether a device with a specified address is reachable, and to examine network connectivity.

The **ping** function is implemented through the Internet Control Message Protocol (ICMP):

Table 87 The source device sends an ICMP echo request to the destination device.

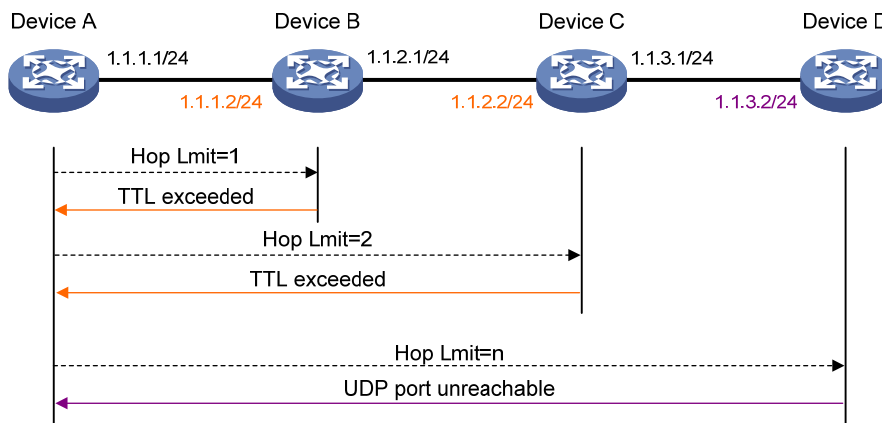
Table 88 The source device determines whether the destination is reachable based on whether it receives an ICMP echo reply. If the destination is reachable, the source device determines the following:

- The link quality, based on the numbers of ICMP echo requests sent and replies received.
- The distance between the source and destination, based on the round trip time of ping packets.

Trace route

By using the **trace route** command, you can trace the Layer 3 devices involved in delivering an IP packet from source to destination to check whether a network is available. This is useful for identification of failed node(s) in the event of network failure.

a. Trace route diagram



The **trace route** function is implemented through ICMP, as shown in a:

Table 89 The source (Device A) sends a packet with a TTL value of 1 to the destination (Device D). The UDP port of the packet is a port number that will not be used by any application of the destination.

Table 90 The first hop (Device B) (the Layer 3 device that first receives the packet) responds by sending a TTL-expired ICMP error message to the source, with its IP address 1.1.1.2 encapsulated. In this way, the source device can get the address (1.1.1.2) of the first Layer 3 device.

Table 91 The source device sends a packet with a TTL value of 2 to the destination device.

Table 92 The second hop (Device C) responds with a TTL-expired ICMP error message, which gives the source device the address (1.1.2.2) of the second Layer 3 device.

Table 93 The process continues until the ultimate destination device is reached. No application of the destination uses this UDP port. The destination replies a port unreachable ICMP error message with the destination IP address 1.1.3.2.

Table 94 When the source device receives the port unreachable ICMP error message, it knows that the packet has reached the destination, and it can get the addresses of all the Layer 3 devices involved to get to the destination device (1.1.1.2, 1.1.2.2, 1.1.3.2).

Diagnostic tool operations

Ping operation

NOTE:

The web interface supports the IPv4 ping operations only.

Select **Network** → **Diagnostic Tools** from the navigation tree to enter the ping configuration page, as shown in [a](#).

a. Ping configuration page

The screenshot shows a web interface for configuring a ping operation. At the top, there are two tabs: 'Ping' and 'Trace Route'. The 'Ping' tab is active. Below the tabs, there is a 'Command' section with a text input field labeled 'Ping' and a 'Start' button. Below that is a 'Summary' section with a large empty rectangular area.

Type in the IPv4 address or the host name of the destination device in the text box, and click **Start** to execute the **ping** command. You will see the result in the **Summary** area, as shown in [b](#).

b. Ping operation result

Summary

```
PING 192.168.1.1: 56 data bytes
  Reply from 192.168.1.1: bytes=56 Sequence=1 ttl=255 time=8 ms
  Reply from 192.168.1.1: bytes=56 Sequence=2 ttl=255 time=11 ms
  Reply from 192.168.1.1: bytes=56 Sequence=3 ttl=255 time=3 ms
  Reply from 192.168.1.1: bytes=56 Sequence=4 ttl=255 time=3 ms
  Reply from 192.168.1.1: bytes=56 Sequence=5 ttl=255 time=3 ms

--- 192.168.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 3/5/11 ms
```

Trace route operation

NOTE:

The web interface supports trace route on IPv4 addresses only.

Before performing the trace route operation on the Web interface, on the intermediate device execute the **ip ttl-expires enable** command to enable the sending of ICMP timeout packets and on the destination device execute the **ip unreachable enable** command to enable the sending of ICMP destination unreachable packets.

Select **Network** → **Diagnostic Tools** from the navigation tree and then select the **Trace Route** tab to enter the trace route configuration page, as shown in [a](#).

a. Trace route configuration page

The screenshot shows a web interface for configuring a trace route. At the top, there are two tabs: "Ping" and "Trace Route", with "Trace Route" being the active tab. Below the tabs, there is a "Command" section with a text input field labeled "Trace Route" and a "Start" button. Below the "Command" section, there is a "Result" section with a large, empty text area for displaying the output of the trace route operation.

Type in the IP address or host name of the destination device in the **Trace Route** text box, and click **Start** to execute the **trace route** command. You will see the output in the **Summary** area, as shown in [b](#).

b. Trace route operation result

Result

```
tracert to 192.168.1.1(192.168.1.1) 30 hops max,40 bytes packet
 1 192.168.1.1 1 ms 2 ms 1 ms
```

ARP management

ARP overview

ARP function

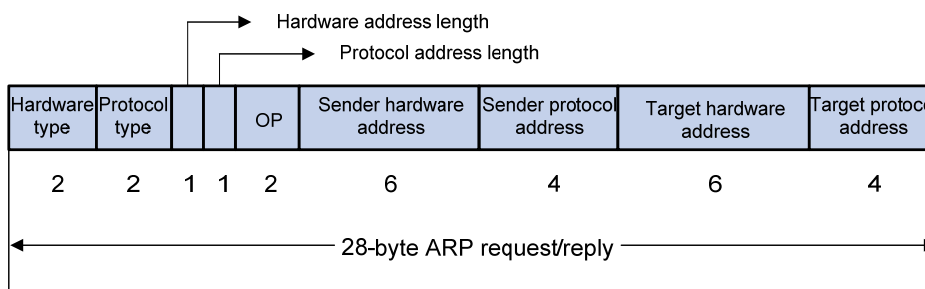
The Address Resolution Protocol (ARP) is used to resolve an IP address into an Ethernet MAC address (or physical address).

In an Ethernet LAN, when a device sends data to another device, it uses ARP to translate the IP address of the destination device to the corresponding MAC address.

ARP message format

ARP messages are classified into ARP requests and ARP replies. **a** shows the format of the ARP request/reply.

a. ARP message format



The following describe the fields in **a**.

- **Hardware type:** This field specifies the hardware address type. The value "1" represents Ethernet.
- **Protocol type:** This field specifies the type of the protocol address to be mapped. The hexadecimal value "0x0800" represents IP.
- **Hardware address length and protocol address length:** They respectively specify the length of a hardware address and a protocol address, in bytes. For an Ethernet address, the value of the hardware address length field is "6". For an IP(v4) address, the value of the protocol address length field is "4".
- **OP:** Operation code. This field specifies the type of the ARP message. The value "1" represents an ARP request and "2" represents an ARP reply.
- **Sender hardware address:** This field specifies the hardware address of the device sending the message.
- **Sender protocol address:** This field specifies the protocol address of the device sending the message.
- **Target hardware address:** This field specifies the hardware address of the device the message is being sent to.

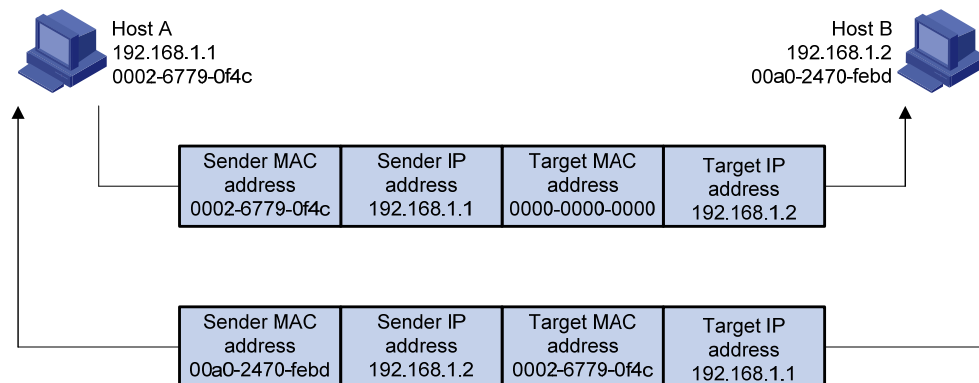
- Target protocol address: This field specifies the protocol address of the device the message is being sent to.

ARP operation

Suppose that Host A and Host B are on the same subnet and Host A sends a packet to Host B, as shown in a. The resolution process is as follows:

- Host A looks into its ARP table to see whether there is an ARP entry for Host B. If yes, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
- If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request, in which the sender IP address and the sender MAC address are the IP address and the MAC address of Host A respectively, and the target IP address and the target MAC address are the IP address of Host B and an all-zero MAC address respectively. Because the ARP request is a broadcast, all hosts on this subnet can receive the request, but only the requested host (Host B) will respond to the request.
- Host B compares its own IP address with the destination IP address in the ARP request. If they are the same, Host B saves the source IP address and source MAC address in its ARP table, encapsulates its MAC address into an ARP reply, and unicasts the reply to Host A.
- After receiving the ARP reply, Host A adds the MAC address of Host B to its ARP table. Meanwhile, Host A encapsulates the IP packet and sends it out.

a. ARP address resolution process



If Host A is not on the same subnet with Host B, Host A first sends an ARP request to the gateway. The target IP address in the ARP request is the IP address of the gateway. After obtaining the MAC address of the gateway from an ARP reply, Host A sends the packet to the gateway. If the gateway maintains the ARP entry of Host B, it forwards the packet to Host B directly; if not, it broadcasts an ARP request, in which the target IP address is the IP address of Host B. After obtaining the MAC address of Host B, the gateway sends the packet to Host B.

ARP table

After obtaining the MAC address for the destination host, the device puts the IP-to-MAC mapping into its own ARP table. This mapping is used for forwarding packets with the same destination in future.

An ARP table contains ARP entries, which fall into one of two categories: dynamic or static.

Dynamic ARP entry

A dynamic entry is automatically created and maintained by ARP. It can get aged, be updated by a new ARP packet, or be overwritten by a static ARP entry. When the aging timer expires or the interface goes down, the corresponding dynamic ARP entry will be removed.

Static ARP entry

A static ARP entry is manually configured and maintained. It cannot get aged or be overwritten by a dynamic ARP entry.

Using static ARP entries enhances communication security. After a static ARP entry is specified, only a specific MAC address is associated with the specified IP address. Attack packets cannot modify the IP-to-MAC mapping. Thus, communications between devices are protected.

Static ARP entries can be classified into long or short.

- A long static ARP entry can be directly used to forward packets. When configuring a long static ARP entry, you must configure a VLAN and an outbound interface for the entry besides the IP address and the MAC address.
- A short static ARP entry has only an IP address and a MAC address configured. It cannot be directly used for forwarding data. If a short static ARP entry matches an IP packet to be forwarded, the device sends an ARP request first. If the sender IP and MAC addresses in the received ARP reply are the same as those in the short static ARP entry, the device adds the interface receiving the ARP reply to the short static ARP entry. Then the entry can be used for forwarding IP packets.

NOTE:

Usually ARP dynamically resolves IP addresses to MAC addresses, without manual intervention.

Managing ARP entries

Displaying ARP entries

Select **Network** → **ARP Management** from the navigation tree to enter the default **ARP Table** page shown in a. All ARP entries are displayed on the page.

a. ARP Table configuration page

	IP Address	MAC Address	VLAN ID	Port	Type	Operation
<input type="checkbox"/>	192.168.0.5	00e0-4c3d-35d7	1	GigabitEthernet1/0/15	Dynamic	
<input type="checkbox"/>	192.168.0.6	0015-e943-712f	1	GigabitEthernet1/0/15	Dynamic	
<input type="checkbox"/>	192.168.0.18	000f-3d80-2b38	1	GigabitEthernet1/0/15	Dynamic	
<input type="checkbox"/>	192.168.0.56	000f-cb00-5601	1	GigabitEthernet1/0/15	Dynamic	

Creating a static ARP entry

Select **Network** → **ARP Management** from the navigation tree to enter the default **ARP Table** page shown in **a**. Click **Add** to enter the **New Static ARP Entry** page. Select the **Advanced Options** checkbox to expand advanced configuration items, as shown in **a**.

a. Add a static ARP entry

2 describes the static ARP entry configuration items.

2. Static ARP entry configuration items

Item	Description
IP Address	Type an IP address for the static ARP entry.
MAC Address	Type a MAC address for the static ARP entry.
Advanced Options	<p>VLAN ID Type a VLAN ID and specify a port for the static ARP entry.</p> <p>⚠ IMPORTANT:</p> <p>Port The VLAN ID must be the ID of the VLAN that has already been created, and the port must belong to the VLAN. The corresponding VLAN interface must have been created.</p>

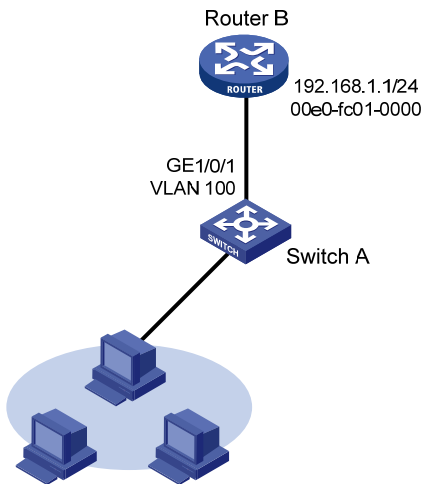
Static ARP configuration example

Network requirements

As shown in **a**, hosts are connected to Switch A, which is connected to Router B through interface GigabitEthernet 1/0/1 belonging to VLAN 100. The IP address of Router B is 192.168.1.1/24. The MAC address of Router B is 00e0-fc01-0000.

To enhance communication security between Switch A and Router B, static ARP entries need to be configured on Switch A.

a. Network diagram for configuring static ARP entries



Configuration procedure

Create VLAN 100.

- Select **Network** → **VLAN** from the navigation tree, click the **Add** tab, and then perform the following operations, as shown in a.

a. Create VLAN 100

Select VLAN **Create** Port Detail Detail Modify VLAN Modify Port Remove

Create:

VLAN IDs: Example:3, 5-10

ID	Description
1	VLAN 0001
999	VLAN 0999

Modify VLAN description (Note: you can do this later on the Modify VLAN page)

Modify the description of the selected VLAN:

ID	Description
<input type="text"/>	<input type="text" value="(1-32 Chars.)"/> <input type="button" value="Apply"/>

- Type **100** for **VLAN ID**.
- Click **Create** to complete the configuration.

Add GigabitEthernet 1/0/1 to VLAN 100.

- Click the **Modify Port** tab and then perform the following operations, as shown in **b**.

b. Add GigabitEthernet 1/0/1 to VLAN 100

Select VLAN Create Port Detail Detail Modify VLAN **Modify Port** Remove

Select Ports

HP V1910-16G Sw...

Select All Select None Not available for

Select membership type:

Untagged Tagged Not A Member Link Type PVID

Enter VLAN IDs to which the port is to be assigned:

VLAN IDs: Example: 1,3,5-10

Selected ports:

Untagged Membership
GE1/0/1

Apply Cancel

- Select interface GigabitEthernet 1/0/1 in the **Select Ports** field.
- Click on the **Untagged** radio button in the **Select membership type** field.
- Type **100** for **VLAN IDs**.
- Click **Apply**. A configuration progress dialog box appears, as shown in **c**.

c. Configuration progress dialog box

Current Configuration

Setting GigabitEthernet1/0/1..... - OK!

100%

Pause Close

- After the configuration process is complete, click **Close**.

Create VLAN-interface 100.

- Select **Network** → **VLAN Interface** from the navigation tree, click the **Create** tab, and then perform the following operations, as shown in [d](#).

d. Create VLAN-interface 100

Summary	Create	Modify	Remove
---------	---------------	--------	--------

Input a VLAN ID:

(1-4094)

Configure Primary IPv4 Address

DHCP BOOTP **Manual**

IPv4 Address: Mask Length: ▾

Configure IPv6 Link Local Address

Auto Manual

IPv6 Address:

- Type **100** for **VLAN ID**.
- Select the **Configure Primary IPv4 Address** checkbox.
- Click on the **Manual** radio button.
- Type **192.168.1.2** for **IPv4 Address**.
- Select **24 (255.255.255.0)** for **Mask Length**.
- Click **Apply** to complete the configuration.

Create a static ARP entry.

- Select **Network** → **ARP Management** from the navigation tree to enter the default **ARP Table** page. Click **Add** Perform the following operations, as shown in [e](#).

e. Create a static ARP entry

ARP Table	Gratuitous ARP
-----------	----------------

New Static ARP Entry

IP Address:	<input type="text" value="192.168.1.1"/>	*
MAC Address:	<input type="text" value="00e0-fc01-0000"/>	*(Example: 0010-dc28-a4e9)
<input checked="" type="checkbox"/>	Advanced Options	
VLAN ID:	<input type="text" value="100"/>	(1-4094)
Port:	<input type="text" value="GigabitEthernet1/0/1"/>	▼

Items marked with an asterisk(*) are required

- Type **192.168.1.1** for **IP Address**.
- Type **00e0-fc01-0000** for **MAC Address**.
- Select the **Advanced Options** checkbox.
- Type **100** for **VLAN ID**.
- Select **GigabitEthernet1/0/1** for **Port**.
- Click **Apply** to complete the configuration.

Gratuitous ARP

Introduction to gratuitous ARP

In a gratuitous ARP packet, the sender IP address and the target IP address are both the IP address of the device issuing the packet, the sender MAC address is the MAC address of the device, and the target MAC address is the broadcast address ff:ff:ff:ff:ff:ff.

A device implements the following functions by sending gratuitous ARP packets:

- Determining whether its IP address is already used by another device.
- Informing other devices about the change of its MAC address so that they can update their ARP entries.

A device receiving a gratuitous ARP packet adds the information carried in the packet to its own dynamic ARP table if it finds no corresponding ARP entry exists in the cache.

An attacker sends spoofed gratuitous ARP packets to hosts on a network. As a result, traffic that the hosts want to send to the gateway is sent to the attacker instead, and the hosts cannot access external networks. To prevent such gateway spoofing attacks, you can enable the gateway to send gratuitous ARP packets periodically. In this way, each host can learn correct gateway address information.

Configuring gratuitous ARP

Select **Network** → **ARP Management** from the navigation tree, and click the **Gratuitous ARP** tab to enter the page shown in a.

a. Gratuitous ARP configuration page

ARP Table

Gratuitous ARP

Gratuitous ARP

Disable gratuitous ARP packets learning function

Send gratuitous ARP packets when receiving ARP requests from another network segments

—Periodical gratuitous ARP packets sending settings

-----Sending Interfaces(Period)

-----Available Interfaces-----

Vlan-interface999

<<

>>

Period ms(200-5000)

Apply

2. Gratuitous ARP configuration items

Item	Description
Disable gratuitous ARP packets learning function	Enable or disable learning of ARP entries according to gratuitous ARP packets. Enabled by default.
Send gratuitous ARP packets when receiving ARP requests from another network segment	Enable the device to send gratuitous ARP packets upon receiving ARP requests from another network segment. Disabled by default.
Periodical gratuitous ARP packets sending settings	<p>Select interfaces for sending gratuitous ARP packets and type the sending period.</p> <p>To add an interface to the Sending Interfaces(Period) list box, select the interface from the Available Interfaces list box, type the sending period, and click the << button.</p> <p>To remove an interface from the Sending Interfaces(Period) list box, select the interface from the list box and click the >> button.</p> <p>⚠ IMPORTANT:</p> <ul style="list-style-type: none"> This function takes effect only when the link of the interface goes up and an IP address has been assigned to the interface. If you change the period for sending gratuitous ARP packets, the configuration is effective at the next sending period.

ARP attack defense configuration

Although ARP is easy to implement, it provides no security mechanism and thus is prone to network attacks. ARP attacks and viruses are threatening LAN security. The device can provide multiple features to detect and prevent such attacks. This chapter mainly introduces these features.

ARP detection

Introduction to ARP detection

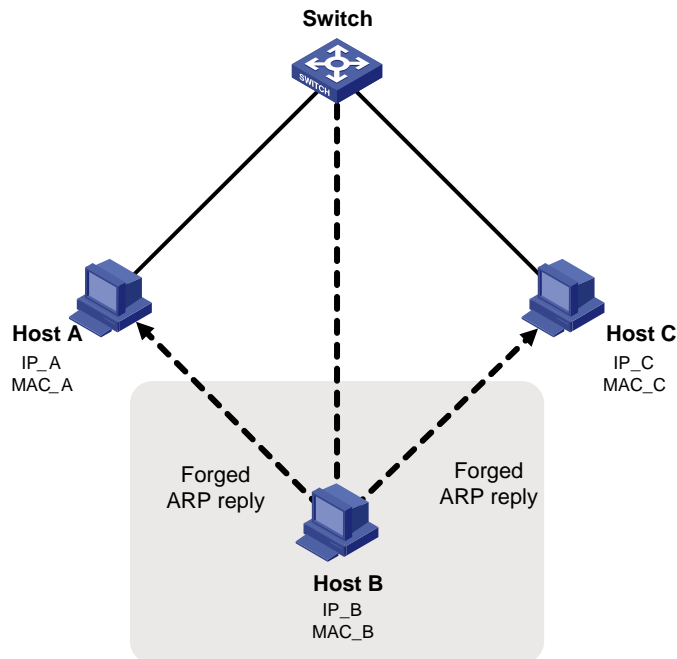
The ARP detection feature allows only the ARP packets of authorized clients to be forwarded, preventing man-in-the-middle attacks.

Man-in-the-middle attack

According to the ARP design, after receiving an ARP reply, a host adds the IP-to-MAC mapping of the sender to its ARP mapping table. This design reduces the ARP traffic on the network, but also makes ARP spoofing possible.

As shown in [a](#), Host A communicates with Host C through a switch. After intercepting the traffic between Host A and Host C, a hacker (Host B) forwards forged ARP replies to Host A and Host C respectively. Upon receiving the ARP replies, the two hosts update the MAC address corresponding to the peer IP address in their ARP tables with the MAC address of Host B (MAC_B). After that, Host B establishes independent connections with Host A and Host C and relays messages between them, deceiving them into believing that they are talking directly to each other over a private connection, while the entire conversation is actually controlled by Host B. Host B may intercept and modify the communication data. Such an attack is called a man-in-the-middle attack.

a. Man-in-the-middle attack



ARP detection mechanism

With ARP detection enabled for a specific VLAN, ARP messages arrived on any interface in the VLAN are redirected to the CPU to have their MAC and IP addresses checked. ARP messages that pass the check are forwarded, and other ARP messages are discarded.

Table 95 ARP detection based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings

With this feature enabled, the device compares the source IP and MAC addresses of an ARP packet received from the VLAN against the DHCP snooping entries, 802.1X security entries, or static IP-to-MAC binding entries. You can specify a detection type or types as needed.

After you enable ARP detection based on DHCP snooping entries for a VLAN,

- Upon receiving an ARP packet from an ARP untrusted port, the device compares the ARP packet against the DHCP snooping entries. If a match is found, that is, the parameters (such as IP address, MAC addresses, port index, and VLAN ID) are consistent, the ARP packet passes the check; if not, the ARP packet cannot pass the check.
- Upon receiving an ARP packet from an ARP trusted port, the device does not check the ARP packet.
- If ARP detection is not enabled for the VLAN, the ARP packet is not checked even if it is received from an ARP untrusted port.

After you enable ARP detection based on 802.1X security entries, the device, upon receiving an ARP packet from an ARP untrusted port, compares the ARP packet against the 802.1X security entries.

- If an entry with identical source IP and MAC addresses, port index, and VLAN ID is found, the ARP packet is considered valid.
- If an entry with no matching IP address but with a matching OUI MAC address is found, the ARP packet is considered valid.

Otherwise, the packet is considered invalid and discarded.

After you enable ARP detection based on static IP-to-MAC bindings, the device, upon receiving an ARP packet from an ARP trusted/untrusted port, compares the source IP and MAC addresses of the ARP packet against the static IP-to-MAC bindings.

- If an entry with a matching IP address but a different MAC address is found, the ARP packet is considered invalid and discarded.
- If an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection.
- If no match is found, the ARP packet is considered valid and can pass the detection.

If all the detection types are specified, the system uses static IP-to-MAC binding entries first, then DHCP snooping entries, and then 802.1X security entries. To prevent gateway spoofing, ARP detection based on IP-to-MAC binding entries is required. After passing this type of ARP detection, users that can pass ARP detection based on DHCP snooping entries or 802.1X security entries are considered to be valid. The last two detection types are used to prevent user spoofing. You can select detection types according to the networking environment.

- If all access clients acquire IP addresses through DHCP, HP recommends that you enable DHCP snooping and ARP detection based on DHCP snooping entries on your access device.
- If access clients are 802.1X clients and large in number, and most of them use static IP addresses, HP recommends that you enable 802.1X authentication, upload of client IP addresses, and ARP detection based on 802.1X security entries on your access device. After that, the access device uses mappings between IP addresses, MAC addresses, VLAN IDs, and ports of 802.1X authentication clients for ARP detection.

If all the detection types are specified, the system uses IP-to-MAC bindings first, then DHCP snooping entries, and then 802.1X security entries. If an ARP packet fails to pass ARP detection based on static IP-to-MAC bindings, it is discarded. If the packet passes this detection, it will be checked against DHCP snooping entries. If a match is found, the packet is considered to be valid and will not be checked against 802.1X security entries; otherwise, the packet is checked against 802.1X security entries. If a match is found, the packet is considered to be valid; otherwise, the packet is discarded.

Table 96 ARP detection based on specified objects

You can also specify objects in 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 both the source and destination IP addresses in an ARP packet. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded. With this object specified, the source and destination IP addresses of ARP replies, and the source IP address of ARP requests are checked.

Configuring ARP detection

NOTE:

If both the ARP detection based on specified objects and the ARP detection based on static IP-to-MAC bindings/DHCP snooping entries/802.1X security entries are enabled, the former one applies first, and then the latter applies.

Select **Network** → **ARP Anti-Attack** from the navigation tree to enter the default **ARP Detection** page shown in a.

a. ARP Detection configuration page

The screenshot shows the ARP Detection configuration page. It includes sections for VLAN Settings, Trusted Ports, User Validation Check, ARP Packet Validation, and Static-Bindings. The Static-Bindings section contains a table with one entry:

	IP	MAC
<input type="checkbox"/>	10.1.1.2	00e0-1234-5678

2. ARP Detection configuration items

Item	Description
VLAN Settings	Select VLANs on which ARP detection is to be enabled. To add VLANs to the Enabled VLAN list box, select one or multiple VLANs from the Disabled VLAN list box and click the << button. To remove VLANs from the Enabled VLAN list box, select one or multiple VLANs from the list box and click the >> button.

Item	Description
Trusted Ports	<p>Select trusted ports.</p> <p>To add ports to the Trusted Ports list box, select one or multiple ports from the Untrusted Ports list box and click the << button.</p> <p>To remove ports from the Trusted Ports list box, select one or multiple ports from the list box and click the >> button.</p>
User Validation Check	<p>Select user validity check modes, including:</p> <ul style="list-style-type: none"> • Using DHCP Snooping to validate users • Using Dot1x to validate users • Using Static-Binding entries to guard against spoofing gateway attack: You can configure static IP-to-MAC bindings if you select this mode. For the detailed configuration, see “Creating a static binding entry”. <p>If all the detection types are specified, the system uses static IP-to-MAC bindings first, then DHCP snooping entries, and then 802.1X security entries. If an ARP packet fails to pass ARP detection based on static IP-to-MAC bindings, it is discarded. If the packet passes this detection, it will be checked against DHCP snooping entries. If a match is found, the packet is considered to be valid and will not be checked against 802.1X security entries; otherwise, the packet is checked against 802.1X security entries. If a match is found, the packet is considered to be valid; otherwise, the packet is discarded.</p> <p>If none of the above is selected, all ARP packets are considered to be invalid.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> • Before enabling ARP detection based on DHCP snooping entries, make sure that DHCP snooping is enabled. • Before enabling ARP detection based on 802.1X security entries, make sure that 802.1X is enabled and the 802.1X clients are configured to upload IP addresses.
ARP Packet Validation	<p>Select ARP packet validity check modes, including:</p> <ul style="list-style-type: none"> • If the source MAC address of an ARP packet is not identical to that in the Ethernet header, the ARP packet is discarded • If the destination MAC address of an ARP reply is all-zero, all-one, or inconsistent with that in the Ethernet header, the ARP packet is discarded • If the source IP address of an ARP request, or the source IP address or destination IP address of an ARP reply is all-zero, all-one or an multicast IP address, the ARP packet is discarded <p>If none of the above is selected, the system does not check the validity of ARP packets.</p>

Creating a static binding entry

If you select **Using Static-Binding entries to guard against spoofing gateway attack**, you can configure static IP-to-MAC binding entries.

To create a static binding entry, type an IP address and MAC address in the **Static Bindings** field, and then click **Add**, as shown in [a](#).

NOTE:

If an entry with a matching IP address but a different MAC address is found, the ARP packet is considered invalid and discarded. If an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection.

802.1X fundamentals

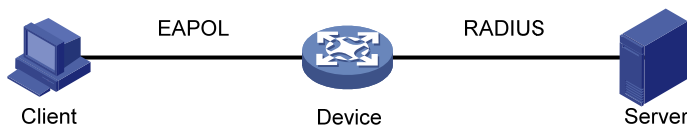
802.1X is a port-based network access control protocol initially proposed by the IEEE 802 LAN/WAN committee for securing wireless LANs (WLANs), and it has also been widely used on Ethernet networks for access control.

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

Architecture of 802.1X

802.1X operates in the client/server model. It comprises three entities: the client (the supplicant), the network access device (the authenticator), and the authentication server, as shown in [a](#).

a. Architecture of 802.1X



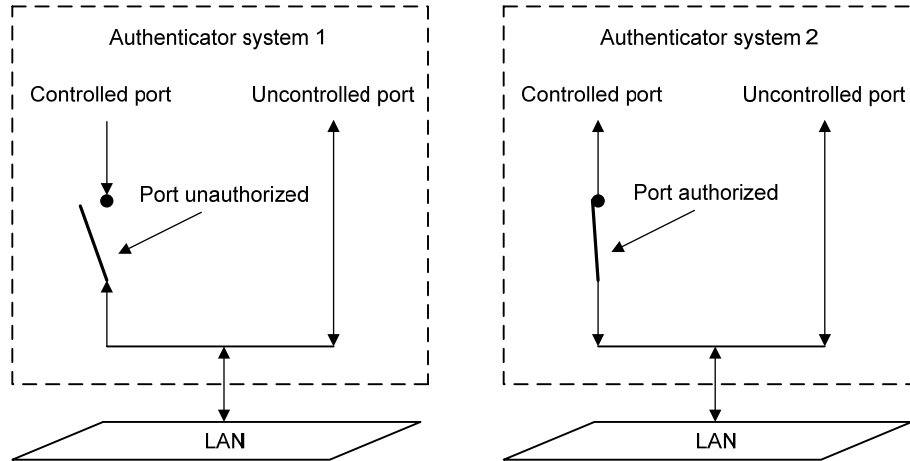
- The client is a user terminal seeking access to the LAN. It must have 802.1X software to authenticate to the network access device.
- The network access device authenticates the client to control access to the LAN. In a typical 802.1X environment, the network access device uses an authentication server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

a. Authorized/unauthorized 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 devices support only unidirectional traffic control.

802.1X-related protocols

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

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

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

NOTE:

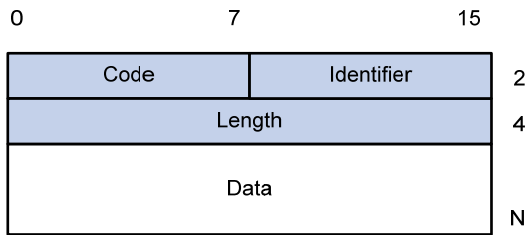
If an 802.1X client uses EAP, the configuration on username format on the device does not take effect. For more information about username format configuration, see the chapter “RADIUS configuration”.

Packet formats

EAP packet format

a shows the EAP packet format.

a. EAP packet format

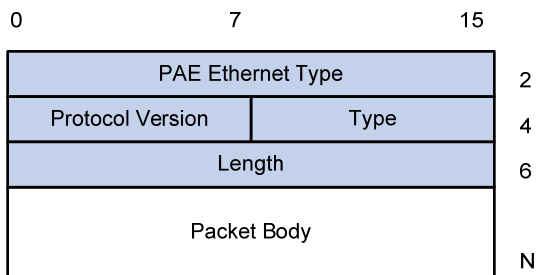


- Code: Type of the EAP packet, which can be Request (1), Response (2), Success (3), or Failure (4).
- Identifier: Used for matching Responses with Requests.
- Length: Length (in bytes) of the EAP packet, which is the sum of the Code, Identifier, Length, and Data fields.
- Data: Content of the EAP packet.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

a shows the EAPOL frame format.

a. EAPOL frame 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. 2 lists the types of EAPOL packets that the HP implementation of 802.1X supports.

2. 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.

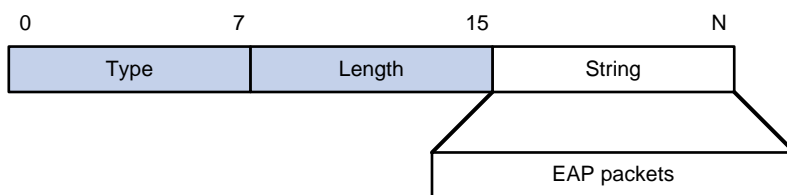
EAP over RADIUS

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

EAP-Message

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

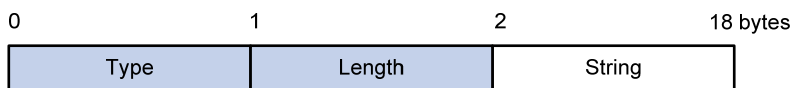
a. EAP-Message attribute format



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.

a. Message-Authenticator attribute format



Initiating 802.1X authentication

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

802.1X client as the initiator

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

Access device as the initiator

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

The access device supports the following modes:

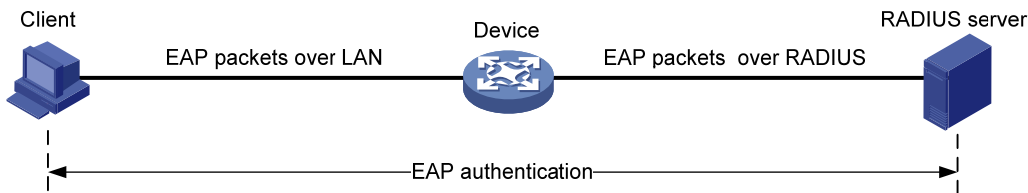
- Multicast trigger mode—The access device multicasts Identity EAP-Request packets periodically (every 30 seconds by default) to initiate 802.1X authentication.
- Unicast trigger mode—Upon receiving a frame with the source MAC address not in the MAC address table, the access device sends an Identity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

802.1X authentication procedures

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

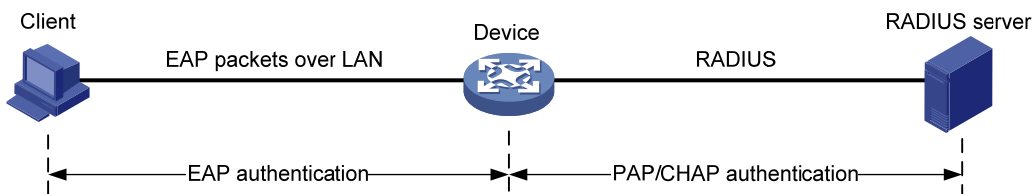
EAP relay is defined in IEEE 802.1X. In this mode, the network device uses EAPoR packets to send authentication information to the RADIUS server, as shown in a.

a. 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 Challenge Handshake Authentication Protocol (CHAP) to authenticate to the RADIUS server, as shown in b.

b. 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 	<p>The RADIUS server must support the EAP-Message and Message-Authenticator attributes, and the EAP authentication method used by the client.</p>

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

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

a. 802.1X authentication procedure in EAP relay mode

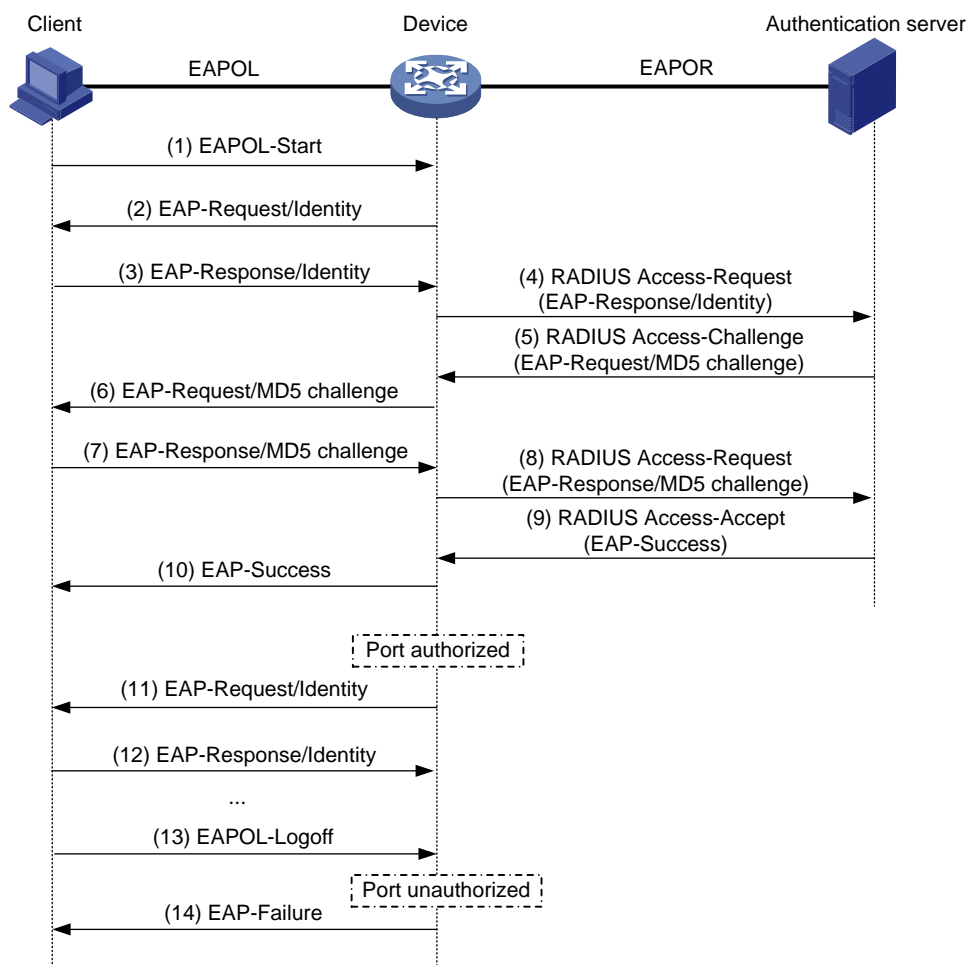


Table 97 When a user launches the 802.1X client software and enters a registered username and password, the 802.1X client software sends an EAPOL-Start packet to the network access device.

Table 98 The network access device responds with an Identity EAP-Request packet to ask for the client username.

Table 99 In response to the Identity EAP-Request packet, the client sends the username in an Identity EAP-Response packet to the network access device.

- Table 100** The network access device relays the Identity EAP-Response packet in a RADIUS Access-Request packet to the authentication server.
- Table 101** 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.
- Table 102** The network access device relays the EAP-Request/MD5 Challenge packet in a RADIUS Access-Request packet to the client.
- Table 103** 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.
- Table 104** The network access device relays the EAP-Response/MD5 Challenge packet in a RADIUS Access-Request packet to the authentication server.
- Table 105** 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.
- Table 106** 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.
- Table 107** 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.
- Table 108** 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.
- Table 109** The client can also send an EAPOL-Logoff packet to ask the network access device for a logoff. Then
- Table 110** 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.

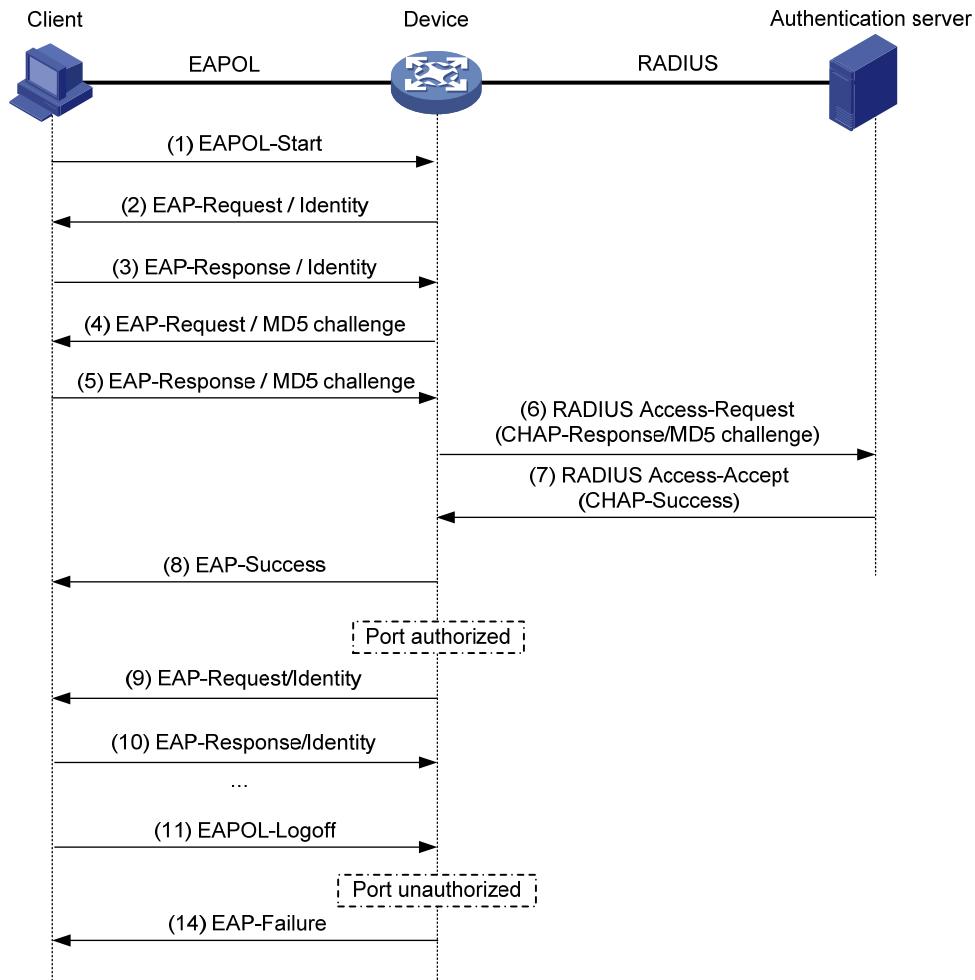
NOTE:

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 configure the EAP relay method.

EAP termination

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

a. 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

HP implementation of 802.1X

This chapter describes how to configure 802.1X on an HP device.

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.

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	<p>Assigns the VLAN to the port as the default VLAN. All subsequent 802.1X users can access the default VLAN without authentication.</p> <p>When the user logs off, the previous default VLAN restores, and all other online users are logged off.</p>
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.• If the port is an access, trunk, or MAC-based VLAN disabled hybrid port, assigns the first authenticated user's VLAN 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.
-

Guest VLAN

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

The device supports guest VLAN on a port that performs port-based access control. The following table describes the way how the device handles VLANs on such port.

Authentication status	VLAN manipulation
No 802.1X user has performed authentication within 90 seconds after 802.1X is enabled or the 802.1X user has failed 802.1X authentication	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. If no 802.1X guest VLAN is configured, the access device does not perform any VLAN operation.
A user in the 802.1X guest VLAN fails 802.1X authentication	The default VLAN on the port is still the 802.1X guest VLAN. All users on the port are in the guest VLAN.
A user in the 802.1X guest VLAN passes 802.1X authentication	<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.

NOTE:

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

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 how to configure RADIUS client and local EAP authentication, see the chapter “AAA configuration”.

802.1X configuration task list

1. 802.1X configuration task list

Task	Description
Configuring 802.1X globally	Required Enable 802.1X authentication globally and configure the authentication method and advanced parameters. By default, 802.1X authentication is disabled globally.
Error! Reference source not found.	Required Enable 802.1X authentication on specified ports and configure 802.1X parameters for the ports. By default, 802.1X authentication is disabled on a port.

Configuring 802.1X globally

From the navigation tree, select **Authentication** → **802.1X** to enter the 802.1X configuration page. In the **802.1X Configuration** area, you can view and configure the 802.1X feature globally.

a. 802.1X configuration page

802.1X Configuration

Enable 802.1X

Authentication Method: CHAP

+Advanced

Apply

Ports With 802.1X Enabled

<input type="checkbox"/>	Port	Port Control	Handshake	Re-Authentication	Max Number of Users	Guest VLAN	Port Authorization	Operation
<input type="checkbox"/>	GigabitEthernet1/0/1	MAC-Based	Enabled	Disabled	256	Disabled	Auto	

Add Del Selected

2. Basic 802.1X configuration items

Item	Description
Enable 802.1X	Enable or disable 802.1X authentication globally.


Item	Description
Authentication Method	<p>Specify the authentication method for 802.1X users. Options include CHAP, PAP, and EAP.</p> <ul style="list-style-type: none"> • CHAP: Sets the access device to perform EAP termination and use the CHAP to communicate with the RADIUS server. • PAP: Sets the access device to perform EAP termination and use the PAP to communicate with the RADIUS server. • EAP: Sets the access device to relay EAP packets, and supports any of the EAP authentication methods to communicate with the RADIUS server. <p>! IMPORTANT:</p> <p>If the client supports only MD5-Challenge EAP authentication, 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.</p> <p>For more information about EAP relay and EAP termination, see "802.1X authentication procedures".</p>

Click **Advanced** to expand the advanced 802.1X configuration area. as shown in a.

3. Advanced 802.1X configuration page

4. Advanced 802.1X configuration items

Item	Description
Quiet	<p>Specify whether to enable the quiet timer.</p> <p>After an 802.1X user fails to be authenticated, the device will keep quiet for a period of time defined by Quiet Period. During the quiet period, the device will not perform 802.1X authentication on the user.</p>
Quiet Period	Specify the value of the quiet timer.
Retry Times	<p>Set the maximum number of authentication request attempts.</p> <p>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 TX Period option or the Supplicant Timeout Time option). The network access device stops retransmitting the request, if it has made the maximum number of request transmission attempts but still received no response.</p>

Item	Description	
TX-Period	<p>Set the username request timeout timer.</p> <p>The timer starts when the device sends an EAP-Request/Identity packet to a client in response to an authentication request. If the device receives no response before this timer expires, it retransmits the request.</p> <p>The timer also sets the interval at which the network device sends multicast EAP-Request/Identity packets to detect clients that cannot actively request authentication.</p>	
Handshake Period	<p>Set the handshake timer.</p> <p>The timer sets the interval at which the access device sends client handshake requests to check the online status of a client that has passed authentication. If the device receives no response after sending the maximum number of handshake requests, it considers that the client has logged off. For information about how to enable the online user handshake function, see "Configuring 802.1X on a port".</p>	
Re-Authentication Period	<p>Set the periodic online user re-authentication timer.</p> <p>The timer sets the interval at which the network device periodically re-authenticates online 802.1X users. The change to the periodic re-authentication timer applies to the users that have been online only after the old timer expires. For information about how to enable periodic online user re-authentication on a port, see "Configuring 802.1X on a port".</p>	
Supplicant Timeout Time	<p>Set the client timeout timer.</p> <p>The 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.</p>	<p> TIP:</p> <p>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.</p>
Server Timeout Time	<p>Set the server timeout timer.</p> <p>The 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.</p>	

NOTE:

Do not change the timer parameters of global 802.1X from their default values unless you have determined that the changes would better the interaction process.

Return to [802.1X configuration task list](#).

Configuring 802.1X on a port

From the navigation tree, select **Authentication** → **802.1X** to enter the 802.1X configuration page, as shown in [a](#). In the **Ports With 802.1X Enabled** area, the 802.1X configuration on ports are listed. Click **Add** to enter the port 802.1X configuration page, as shown in [a](#).

a. 802.1X configuration on a port

802.1X

Apply 802.1X Port Configuration

Port	GigabitEthernet1/0/1 ▼	
Port Control	MAC Based ▼	
Port Authorization	Auto ▼	
Max Number of Users	256 *(1-256, Default = 256)	
Handshake	<input checked="" type="checkbox"/> Enable Handshake	
Re-Authentication	<input type="checkbox"/> Enable Re-Authentication	
Guest VLAN	<input type="checkbox"/> Enable Guest VLAN	VLAN ID <input type="text"/> (1-4094)

Items marked with an asterisk(*) are required

Apply
Cancel

2. Port 802.1X configuration items

Item	Description
Port	<p>Select the port to be enabled with 802.1X authentication. Only 802.1X-disabled ports are available.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> • If the PVID of a port is the same as a voice VLAN, the 802.1X function cannot take effect on the port. • 802.1X is mutually exclusive with link aggregation configuration on a port.
Port Control	<p>Select the access control method for the port, which can be MAC Based or Port Based.</p>
Port Authorization	<p>Select the port authorization state for 802.1X.</p> <p>Options include:</p> <ul style="list-style-type: none"> • 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. • Force-Authorized—Places the port in the authorized state, enabling users on the port to access the network without authentication. • Force-Unauthorized—Places the port in the unauthorized state, denying any access requests from users on the port.
Max Number of Users	<p>Set the maximum number of concurrent 802.1X users on the port.</p>

Item	Description
HandShake	<p>Specify whether to enable the online user handshake function.</p> <p>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 Handshake Period setting. If no response is received from an online user after the maximum number of handshake attempts (set by the Retry Times setting) has been made, the network access device sets the user in the offline state. For information about the timers, see 4.</p> <p>! IMPORTANT:</p> <p>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.</p>
Enable Re-authentication	<p>Specify whether to enable periodic online user re-authentication on the port.</p> <p>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, and VLAN. The re-authentication interval is specified by the Re-Authentication Period setting in 4.</p>
Guest VLAN	<p>Specify an existing VLAN as the guest VLAN. For more information, see "Configuring an 802.1X guest VLAN."</p>

Return to [802.1X configuration task list](#).

Configuring an 802.1X guest VLAN

Table 111 Configuration guidelines

- You can configure only one 802.1X guest VLAN on a port. The 802.1X guest VLANs on different ports can be different.
- Assign different IDs for the voice VLAN, default VLAN, and 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.

Table 112 Configuration prerequisites

- Create the VLAN to be specified as the 802.1X guest VLAN.
- On the 802.1X-enabled port that performs port-based access control, enable 802.1X multicast trigger at the command line interface. (802.1X multicast trigger is enabled by default.)

Configuration examples

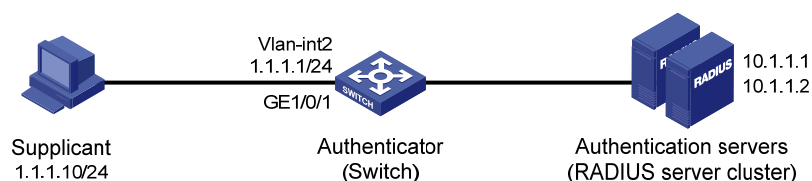
802.1X configuration example

Network requirements

- As shown in [a](#), it is required to perform 802.1X authentication on port GigabitEthernet 1/0/1 to control user access to the Internet, configure the access control method as MAC address based on the port, and enable periodic re-authentication of online users on the port, so that the server can periodically update the authorization information of the users.

- All users belong to default domain **test**. RADIUS authentication is performed. If RADIUS accounting fails, the switch gets the corresponding user offline. The RADIUS servers run iMC.
- A server group with two RADIUS servers is connected to the switch. The IP addresses of the servers are 10.1.1.1 and 10.1.1.2 respectively. Use the former as the primary authentication/secondary accounting server, and the latter as the secondary authentication/primary accounting server.
- Set the shared key for the device to exchange packets with the authentication server as **name**, and that for the device to exchange packets with the accounting server as **money**.
- Specify the device to try up to five times at an interval of 5 seconds in transmitting a packet to the RADIUS server until it receives a response from the server, and to send real time accounting packets to the accounting server every 15 minutes.
- Specify the device to remove the domain name from the username before passing the username to the RADIUS server.

a. **Network diagram for 802.1X configuration**



Configuration procedure

NOTE:

The following configuration procedure involves RADIUS client configuration for the switch, while configurations on the RADIUS servers are omitted. For information about RADIUS configuration, see chapter "RADIUS configuration."

Table 113 Configure the IP addresses of the interfaces. (omitted)

Table 114 Configure 802.1X.

Enable 802.1X globally.

- From the navigation tree, select **Authentication** → **802.1X** to enter the 802.1X configuration page.

b. Global 802.1X configuration

802.1X

802.1X Configuration

Enable 802.1X

Authentication Method

+Advanced

Apply

Ports With 802.1X Enabled

<input type="checkbox"/>	Port	Port Control	Handshake	Re-Authentication	Max Number of Users	Guest VLAN	Port Authorization	Operation

Add Del Selected

- Select the check box before **Enable 802.1X**.
- Select the authentication method as CHAP.
- Click **Apply** to finish the operation.

Enable and configure 802.1X on port GigabitEthernet 1/0/1.

- In the **Ports With 802.1X Enabled** area, click **Add**.

c. 802.1X configuration of GigabitEthernet 1/0/1

802.1X

Apply 802.1X Port Configuration

Port	<input type="text" value="GigabitEthernet1/0/1"/>
Port Control	<input type="text" value="MAC Based"/>
Port Authorization	<input type="text" value="Auto"/>
Max Number of Users	<input type="text" value="256"/> *(1-256, Default = 256)
Handshake	<input checked="" type="checkbox"/> Enable Handshake
Re-Authentication	<input checked="" type="checkbox"/> Enable Re-Authentication
Guest VLAN	<input type="checkbox"/> Enable Guest VLAN VLAN ID <input type="text"/> (1-4094)

Items marked with an asterisk(*) are required

Apply Cancel

- Select port **GigabitEthernet1/0/1** from the port drop-down list.
- Select the checkbox before **Enable Re-Authentication**.
- Click **Apply** to finish the operation.

Table 115 Configure the RADIUS scheme **system**.

Configure the RADIUS authentication servers.

- From the navigation tree, select **Authentication** → **RADIUS**. The RADIUS server configuration page appears.

d. RADIUS authentication server configuration

RADIUS Server	RADIUS Setup
Server Type:	Authentication Server
Primary Server IP:	10.1.1.1 *
Primary Server UDP Port:	1812 *(1-65535)
Primary Server Status:	active
Secondary Server IP:	10.1.1.2 *
Secondary Server UDP Port:	1812 *(1-65535)
Secondary Server Status:	active

Items marked with an asterisk(*) are required

Apply

- Select **Authentication Server** as the server type.
- Enter the primary server IP address 10.1.1.1.
- Select **active** as the primary server's status.
- Enter the secondary server IP address 10.1.1.2.
- Select **active** as the secondary server's status.
- Click **Apply**.

Configure the RADIUS accounting servers.

e. RADIUS accounting server configuration

RADIUS Server	RADIUS Setup
Server Type:	Accounting Server
Primary Server IP:	10.1.1.2 *
Primary Server UDP Port:	1813 *(1-65535)
Primary Server Status:	active
Secondary Server IP:	10.1.1.1 *
Secondary Server UDP Port:	1813 *(1-65535)
Secondary Server Status:	active

Items marked with an asterisk(*) are required

Apply

- Select **Accounting Server** as the server type.

- Enter the primary server IP address 10.1.1.2.
- Select **active** as the primary server's status.
- Enter the secondary server IP address 10.1.1.1.
- Select **active** as the secondary server's status.
- Click **Apply** to finish the operation.

Configure the scheme used for communication between the device and the RADIUS servers.

- Select the **RADIUS Setup** tab to enter the RADIUS parameter configuration page.

f. RADIUS parameter configuration

RADIUS Server		RADIUS Setup	
Server Type:	extended		
<input checked="" type="checkbox"/> Authentication Server Shared Key:	(1-64 Chars.)	
Confirm Authentication Shared Key:		
<input checked="" type="checkbox"/> Accounting Server Shared Key:	(1-64 Chars.)	
Confirm Accounting Shared Key:		
NAS-IP:			
Timeout Interval:	5	*seconds(1-10)	
Timeout Retransmission Times:	5	*(1-20)	
Realtime-Accounting Interval:	15	*minutes(0-60, Must be a multiple of 3)	
Realtime-Accounting Packet Retransmission Times:	5	*(1-255)	
Stop-Accounting Buffer:	enable		
Stop-Accounting Packet Retransmission Times:	500	*(10-65535)	
Quiet Interval:	5	*minutes(1-255)	
Username Format:	with-domain		
Unit of Data Flows:	byte		
Unit of Packets:	packet		

Items marked with an asterisk(*) are required

- Select **extended** as the server type.
- Select the **Authentication Server Shared Key** checkbox, and enter **name** in the textbox.
- Enter **name** again in the **Confirm Authentication Shared Key** textbox.
- Select the **Accounting Server Shared Key** checkbox, and enter **money** in the textbox.
- Enter **money** again in the **Confirm Accounting Shared Key** textbox.
- Enter **5** in the **Timeout Interval** textbox
- Enter **5** in the **Timeout Retransmission Times** textbox.
- Enter **15** in the **Realtime-Accounting Interval** textbox.
- Click **Apply** to finish the operation.

Table 116 Configure AAA

Create an ISP domain.

- From the navigation tree, select **Authentication** → **AAA**. The domain setup page appears.

g. Create an ISP domain

Domain Setup Authentication Authorization Accounting

ISP Domain

Domain Name test (1 - 24 Chars.)

Default Domain Enable

Apply

Please select the ISP domain(s)

Domain Name	Default Domain
system	Default

Select All Select None Remove

- Enter **test** in the **Domain Name** textbox.
- Select **Enable** to use the domain as the default domain.
- Click **Apply** to finish the operation.

Configure the AAA authentication method for the ISP domain.

- Select the **Authentication** tab.

h. Configure the AAA authentication method for the ISP domain

Domain Setup Authentication Authorization Accounting

Authentication Configuration of AAA

Select an ISP domain test

Default AuthN RADIUS Name system Secondary Method

LAN-access AuthN Name Secondary Method

Login AuthN Name Secondary Method

PPP AuthN Name Secondary Method

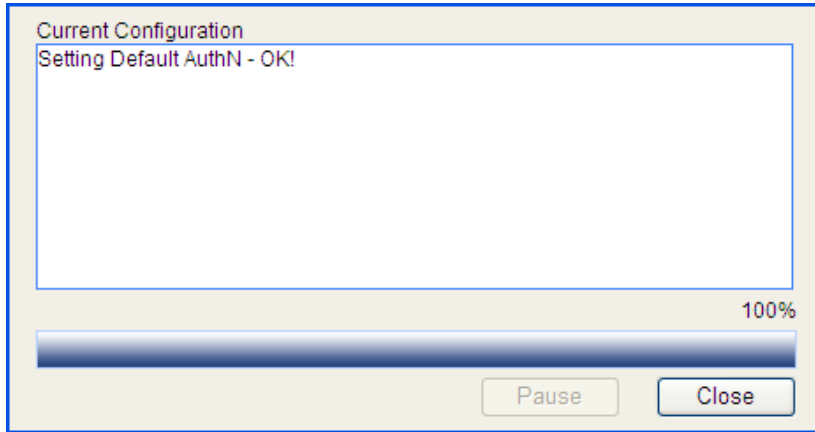
Portal AuthN Name Secondary Method

Apply

- Select the domain name **test**.

- Select the **Default AuthN** checkbox and then select **RADIUS** as the authentication mode.
- Select **system** from the **Name** drop-down list to use it as the authentication scheme.
- Click **Apply**. A configuration progress dialog box appears, as shown in i.

i. **Configuration progress dialog box**

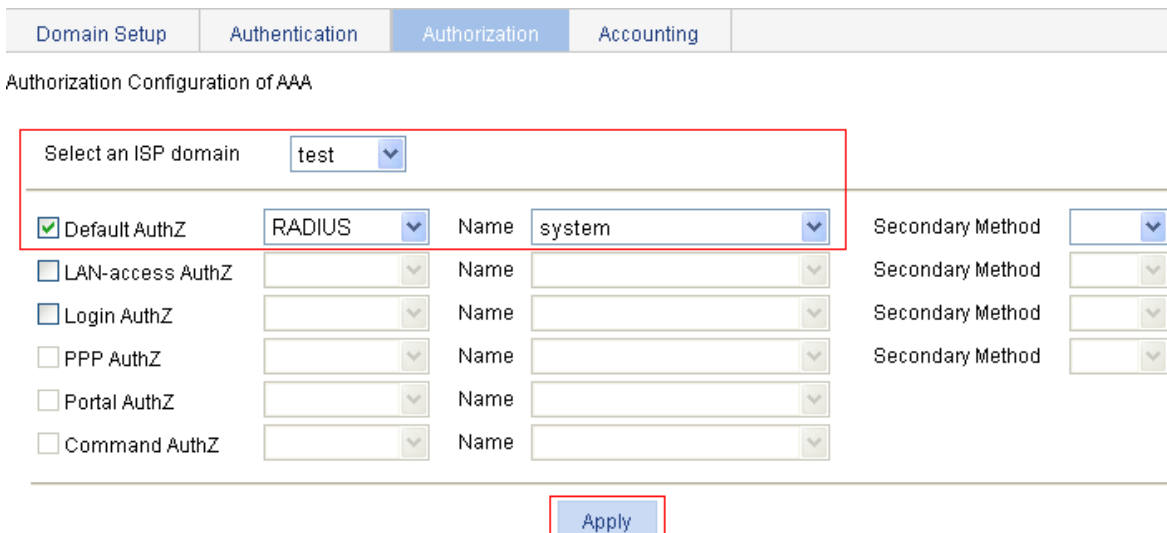


- After the configuration process is complete, click **Close**.

Configure the AAA authorization method for the ISP domain.

- Select the **Authorization** tab.

j. **Configure the AAA authorization method for the ISP domain**



- Select the domain name **test**.
- Select the **Default AuthZ** checkbox and then select **RADIUS** as the authorization mode.
- Select **system** from the **Name** drop-down list to use it as the authorization scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

Configure the AAA accounting method for the ISP domain.

- Select the **Accounting** tab.

k. Configure the AAA accounting method for the ISP domain

Domain Setup	Authentication	Authorization	Accounting	
--------------	----------------	---------------	------------	--

Accounting Configuration of AAA

Select an ISP domain:

Accounting Optional:

Default Accounting: Name: Secondary Method:

LAN-access Accounting: Name: Secondary Method:

Login Accounting: Name: Secondary Method:

PPP Accounting: Name: Secondary Method:

Portal Accounting: Name:

- Select the domain name **test**.
- Select the **Default Accounting** checkbox and then select **RADIUS** as the accounting mode.
- Select **system** from the **Name** drop-down list to use it as the accounting scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

ACL assignment configuration example

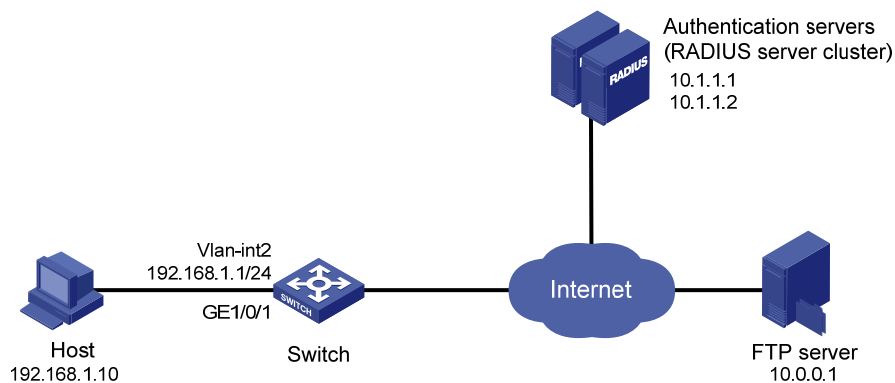
Network requirements

As shown in a, the switch and the RADIUS authentication servers (iMC servers) work together to authenticate the host that is to access the Internet. An FTP server is on the Internet, and its IP address is 10.0.0.1.

- Configure the authentication server to assign ACL 3000.
- Enable 802.1X on port GigabitEthernet 1/0/1 and configure ACL 3000 on the switch.

After a user passes 802.1X authentication, the authentication server assigns ACL 3000. At this time, ACL 3000 takes effect on GigabitEthernet 1/0/1, allowing the host to access the Internet but not the FTP server.

a. Network diagram for ACL assignment



Configuration procedure

Table 117 Configure the IP addresses of the interfaces. (Omitted)

Table 118 Configure the RADIUS scheme **system**

Configure the RADIUS authentication server.

- From the navigation tree, select **Authentication** → **RADIUS**. The RADIUS server configuration page appears.

b. RADIUS authentication server configuration

RADIUS Server	RADIUS Setup
Server Type:	Authentication Server ▼
Primary Server IP:	10.1.1.1 *
Primary Server UDP Port:	1812 *(1-65535)
Primary Server Status:	active ▼
Secondary Server IP:	0.0.0.0 *
Secondary Server UDP Port:	1812 *(1-65535)
Secondary Server Status:	block ▼

Items marked with an asterisk(*) are required

Apply

- Select **Authentication Server** as the server type.
- Enter the primary server IP address 10.1.1.1.
- Enter the primary server UDP port number 1812.
- Select **active** as the primary server status.
- Click **Apply**.

Configure the RADIUS accounting server.

c. RADIUS accounting server configuration

RADIUS Server	RADIUS Setup
Server Type:	Accounting Server ▼
Primary Server IP:	10.1.1.2 *
Primary Server UDP Port:	1813 *(1-65535)
Primary Server Status:	active ▼
Secondary Server IP:	0.0.0.0 *
Secondary Server UDP Port:	1813 *(1-65535)
Secondary Server Status:	block ▼

Items marked with an asterisk(*) are required

Apply

- Select **Accounting Server** as the server type.
- Enter the primary server IP address 10.1.1.2.
- Enter the primary server UDP port number 1813.
- Select **active** as the primary server status.
- Click **Apply** to finish the operation.

Configure the scheme to be used for communication between the switch and the RADIUS servers.

- Select the **RADIUS Setup** tab to enter the RADIUS parameter configuration page.

d. RADIUS parameter configuration

- Select **extended** as the server type.
- Select the **Authentication Server Shared Key** checkbox, and enter **abc** in the textbox.
- Enter **abc** again in the **Confirm Authentication Shared Key** textbox.
- Select the **Accounting Server Shared Key** checkbox, and enter **abc** in the textbox.
- Enter **abc** again in the **Confirm Accounting Shared Key** textbox.
- Select **without-domain** as the username format.
- Click **Apply** to finish the operation.

Table 119 Configure AAA

Create an ISP domain.

- From the navigation tree, select **Authentication** → **AAA**. The domain setup page appears.

e. Create an ISP domain

Domain Setup Authentication Authorization Accounting

ISP Domain

Domain Name test (1 - 24 Chars.)

Default Domain Enable

Apply

Please select the ISP domain(s)

Domain Name	Default Domain
system	Default

Select All Select None Remove

- Enter **test** in the **Domain Name** textbox.
- Select **Enable** to use the domain the default domain.
- Click **Apply** to finish the operation.

Configure the AAA authentication method for the ISP domain.

- Select the **Authentication** tab.

f. Configure the AAA authentication method for the ISP domain

Domain Setup Authentication Authorization Accounting

Authentication Configuration of AAA

Select an ISP domain test

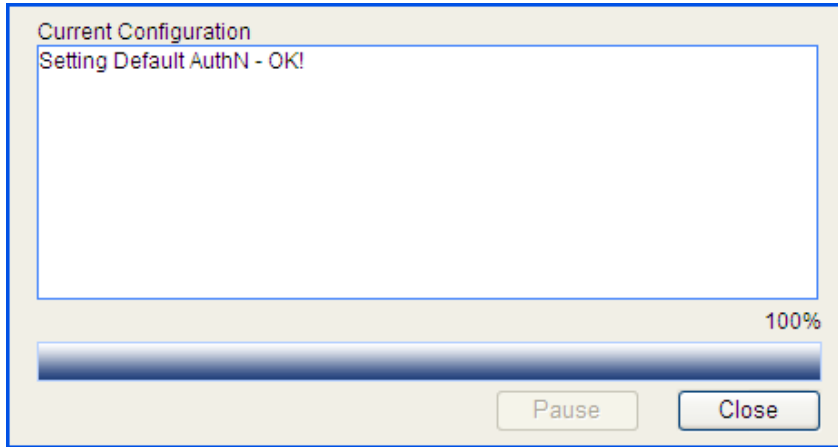
<input checked="" type="checkbox"/> Default AuthN	RADIUS	Name system	Secondary Method
<input type="checkbox"/> LAN-access AuthN		Name	Secondary Method
<input type="checkbox"/> Login AuthN		Name	Secondary Method
<input type="checkbox"/> PPP AuthN		Name	Secondary Method
<input type="checkbox"/> Portal AuthN		Name	Secondary Method

Apply

- Select the domain name **test**.

- Select the **Default AuthN** checkbox and then select **RADIUS** as the authentication mode.
- Select **system** from the **Name** drop-down list to use it as the authentication scheme.
- Click **Apply**. A configuration progress dialog box appears, as shown in g.

g. Configuration progress dialog box



- After the configuration process is complete, click **Close**.
- # Configure the AAA authorization method for the ISP domain.

- Select the **Authorization** tab.

h. Configure the AAA authorization method for the ISP domain

Domain Setup	Authentication	Authorization	Accounting
Authorization Configuration of AAA			
Select an ISP domain: test			
<input checked="" type="checkbox"/> Default AuthZ	RADIUS	Name: system	Secondary Method: []
<input type="checkbox"/> LAN-access AuthZ	[]	Name: []	Secondary Method: []
<input type="checkbox"/> Login AuthZ	[]	Name: []	Secondary Method: []
<input type="checkbox"/> PPP AuthZ	[]	Name: []	Secondary Method: []
<input type="checkbox"/> Portal AuthZ	[]	Name: []	Secondary Method: []
<input type="checkbox"/> Command AuthZ	[]	Name: []	Secondary Method: []
Apply			

- Select the domain name **test**.
 - Select the **Default AuthZ** checkbox and then select **RADIUS** as the authorization mode.
 - Select **system** from the **Name** drop-down list to use it as the authorization scheme.
 - Click **Apply**. A configuration progress dialog box appears.
 - After the configuration process is complete, click **Close**.
- # Configure the AAA accounting method for the ISP domain, and enable accounting optional.
- Select the **Accounting** tab.

i. Configure the AAA accounting method for the ISP domain

Domain Setup	Authentication	Authorization	Accounting
--------------	----------------	---------------	------------

Accounting Configuration of AAA

Select an ISP domain:

Accounting Optional:

Default Accounting: Name: Secondary Method:

LAN-access Accounting: Name: Secondary Method:

Login Accounting: Name: Secondary Method:

PPP Accounting: Name: Secondary Method:

Portal Accounting: Name:

- Select the domain name **test**.
- Select the **Accounting Optional** checkbox, and then select **Enable** for this parameter.
- Select the **Default Accounting** checkbox and then select **RADIUS** as the accounting mode.
- Select **system** from the **Name** drop-down list to use it as the accounting scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

Table 120 Configure an ACL.

Create ACL 3000 that denies packets with destination IP address 10.0.0.1.

- From the navigation tree, select **QoS** → **ACL IPv4** to enter the IPv4 ACL configuration page, and then select the **Create** tab.

j. Create ACL 3000

Summary	Create	Basic Setup	Advanced Setup	Link Layer Setup	Remove
---------	--------	-------------	----------------	------------------	--------

ACL Number: 2000-2999 for basic ACLs.
3000-3999 for advanced ACLs.
4000-4999 for Ethernet frame header ACLs.

Match Order:

ACL Number	Type	Number of Rules	Match Order

- Enter 3000 as the ACL number.
- Click **Apply** to finish the operation.

Configure the ACL to deny packets with destination IP address 10.0.0.1.

- Select the **Advanced Setup** tab.

k. ACL rule configuration

Summary	Create	Basic Setup	Advanced Setup	Link Layer Setup	Remove
---------	--------	-------------	----------------	------------------	--------

ACL Help

Configure an Advanced ACL

Rule ID (0-65534, If no ID is entered, the system will specify one.)

Action

Non-first Fragments Only Logging

IP Address Filter

Source IP Address Source Wildcard

Destination IP Address Destination Wildcard

Protocol

ICMP Type

ICMP Message

ICMP Type (0-255) ICMP Code (0-255)

TCP/UDP Port

TCP Connection

Established

Source: Operator Port -

Destination: Operator Port -

(Range of Port is 0-65535)

Precedence Filter

DSCP

TOS Precedence

Time Range

Add

Rule ID	Operation	Description	Time Range
---------	-----------	-------------	------------

- Select 3000 from the **Select Access Control List(ACL)** drop-down list.
- Select the **Rule ID** check box, and enter 0 as the rule ID.

- Select **Deny** as the operation action.
- In the **IP Address Filter** area, select the **Destination IP Address** check box, and enter 10.0.0.1 in the text box.
- Enter 0.0.0.0 in the **Destination Wildcard** text box.
- Click **Add** to finish the operation.

Table 121 Configure the 802.1X feature.

Enable the 802.1X feature globally.

- From the navigation tree, select **Authentication** → **802.1X** to enter the 802.1X configuration page.

I. Global 802.1X globally

802.1X

802.1X Configuration

Enable 802.1X

Authentication Method

+Advanced

[Apply](#)

Ports With 802.1X Enabled

<input type="checkbox"/>	Port	Port Control	Handshake	Re-Authentication	Max Number of Users	Guest VLAN	Port Authorization	Operation
Add Del Selected								

- Select the check box before **Enable 802.1X**.
- Select the authentication method as CHAP.
- Click **Apply** to finish the operation.

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

- In the **Ports With 802.1X Enabled** area, click **Add**.

m. 802.1X configuration of GigabitEthernet 1/0/1

802.1X

Apply 802.1X Port Configuration

Port	GigabitEthernet1/0/1	▼
Port Control	MAC Based	▼
Port Authorization	Auto	▼
Max Number of Users	256	*(1-256, Default = 256)
Handshake	<input checked="" type="checkbox"/> Enable Handshake	
Re-Authentication	<input type="checkbox"/> Enable Re-Authentication	
Guest VLAN	<input type="checkbox"/> Enable Guest VLAN	VLAN ID <input type="text"/> (1-4094)

Items marked with an asterisk(*) are required

- Select **GigabitEthernet1/0/1** from the port list.
- Click **Apply** to finish the operation.

Configuration verification

After the user passes authentication and gets online, use the **ping** command to test whether ACL 3000 takes effect.

- From the navigation tree, select **Network** → **Diagnostic Tools**. The ping page appears.
- Enter the destination IP address 10.0.0.1.
- Click **Start** to start the ping operation.
- **α** shows the ping operation summary.

a. Ping operation summary

Summary

```
PING 10.0.0.1: 56 data bytes
  Request time out
  Request time out
  Request time out
  Request time out
  Request time out

--- 10.0.0.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
 100.00% packet loss
```

AAA configuration

Overview

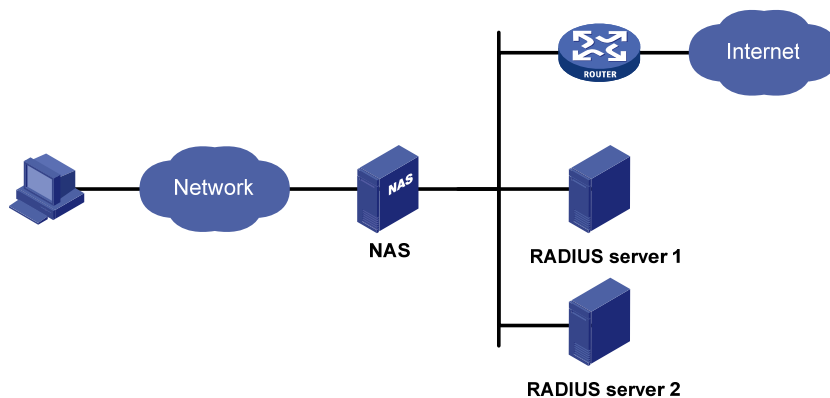
Introduction to AAA

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

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

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

[a](#). Network diagram for AAA



When a user tries to log in to the NAS, use the 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 protocol defines how a NAS and a remote server exchange user information between them.

In the network shown in [a](#), there are two RADIUS servers. You can choose different servers for different security functions. For example, you can use RADIUS server 1 for authentication and authorization, and RADIUS server 2 for accounting.

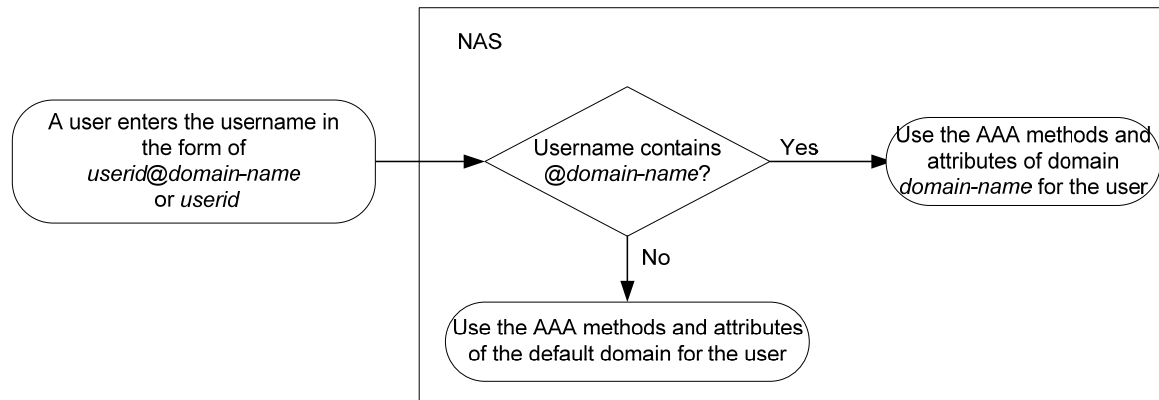
You can choose the three security functions provided by AAA as required. For example, if your company only wants employees to be authenticated before they access specific resources, you only need to configure an authentication server. If network usage information is needed, you must also configure an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

AAA can be implemented through multiple protocols. The switch supports using RADIUS, which is the most commonly used protocol in practice. For more information, see the chapter “RADIUS configuration.”

Domain-based user management

On a NAS, each user belongs to one Internet service provider (ISP) domain. A NAS determines the ISP domain a user belongs to by the username entered by the user at login, and controls access of the user based on the AAA methods configured for the domain. If no specific AAA methods are configured for the domain, the default methods are used. See [a](#).

a. Determine the ISP domain of a user by the username



Configuring AAA

Configuration prerequisites

To implement local user authentication, authorization, and accounting, you must create local users and configure user attributes on the switch. See the chapter “User configuration”.

To implement remote authentication, authorization, or accounting, you must create the RADIUS schemes to be referenced. For RADIUS scheme configuration information, see the chapter “RADIUS configuration”.

Configuration task list

Task	Remarks
Configuring an ISP domain	Optional Create ISP domains and specify one of them as the default ISP domain. By default, there is a system predefined ISP domain named system , which is the default ISP domain.

Task	Remarks
Configuring authentication methods for the ISP domain	<p>Optional</p> <p>Configure authentication methods for various types of users.</p> <p>By default, all types of users use local authentication.</p>
Configuring authorization methods for the ISP domain	<p>Optional</p> <p>Specify the authorization methods for various types of users.</p> <p>By default, all types of users use local authorization.</p>
Configuring accounting methods for the ISP domain	<p>Required</p> <p>Specify the accounting methods for various types of users.</p> <p>By default, all types of users use local accounting.</p>

AAA user types include LAN users (such as 802.1X authentication users and MAC authentication users), login users (such as SSH, Telnet, FTP, terminal access users), and command users.

Configuring an ISP domain

Select **Authentication** → **AAA** from the navigation tree. The **Domain Setup** page appears, as shown in a.

a. Domain Setup page

Domain Setup
Authentication
Authorization
Accounting

ISP Domain

Domain Name (1 - 24 Chars.)

Default Domain

Please select the ISP domain(s)

Domain Name	Default Domain
system	Default

2. ISP domain configuration items

Item	Description
Domain Name	Type the ISP domain name, which is for identifying the domain. You can type a new domain name to create a domain, or specify an existing domain to change its status (whether it is the default domain).
Default Domain	Specify whether to use the ISP domain as the default domain. <ul style="list-style-type: none"> • Enable: Uses the domain as the default domain. • Disable: Uses the domain as a non-default domain. There can only be one default domain at a time. If you specify a second domain as the default domain, the original default domain becomes a non-default domain.

Return to [Configuration task list](#).

Configuring authentication methods for the ISP domain

Select **Authentication** → **AAA** from the navigation tree and then select the **Authentication** tab to enter the authentication method configuration page, as shown in [a](#).

a. Authentication method configuration page

Domain Setup

Authentication

Authorization

Accounting

Authentication Configuration of AAA

Select an ISP domain system ▼

<input type="checkbox"/> Default AuthN	Local ▼	Name ▼	Secondary Method ▼
<input type="checkbox"/> LAN-access AuthN	 ▼	Name ▼	Secondary Method ▼
<input type="checkbox"/> Login AuthN	 ▼	Name ▼	Secondary Method ▼
<input type="checkbox"/> PPP AuthN	 ▼	Name ▼	Secondary Method ▼
<input type="checkbox"/> Portal AuthN	 ▼	Name ▼	

Apply

2. Authentication method configuration items

Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Default AuthN	Configure the default authentication method and secondary authentication method for all types of users.
Name	Options include: <ul style="list-style-type: none"> • Local—Performs local authentication. • None—All users are trusted and no authentication is performed. Generally, this mode is not recommended.
Secondary Method	<ul style="list-style-type: none"> • RADIUS—Performs RADIUS authentication. You must specify the RADIUS scheme to be used. • Not Set—Restore the default, that is, local authentication.

Item	Description
LAN-access AuthN	Configure the authentication method and secondary authentication method for LAN users.
Name	Options include: <ul style="list-style-type: none"> Local—Performs local authentication. None—All users are trusted and no authentication is performed. For security, do not use this mode whenever possible.
Secondary Method	<ul style="list-style-type: none"> RADIUS—Performs RADIUS authentication. You must specify the RADIUS scheme to be used. Not Set—Uses the default authentication methods.
Login AuthN	Configure the authentication method and secondary authentication method for login users.
Name	Options include: <ul style="list-style-type: none"> Local—Performs local authentication. None—All users are trusted and no authentication is performed. Generally, this mode is not recommended.
Secondary Method	<ul style="list-style-type: none"> RADIUS—Performs RADIUS authentication. You must specify the RADIUS scheme to be used. Not Set—Uses the default authentication methods.

Return to [Configuration task list](#).

Configuring authorization methods for the ISP domain

Select **Authentication** → **AAA** from the navigation tree and then select the **Authorization** tab to enter the authorization method configuration page, as shown in [a](#).

a. Authorization method configuration page

Domain Setup	Authentication	Authorization	Accounting
--------------	----------------	---------------	------------

Authorization Configuration of AAA

Select an ISP domain:

<input type="checkbox"/> Default AuthZ	<input type="text" value="Local"/>	Name <input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> LAN-access AuthZ	<input type="text"/>	Name <input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> Login AuthZ	<input type="text"/>	Name <input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> PPP AuthZ	<input type="text"/>	Name <input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> Portal AuthZ	<input type="text"/>	Name <input type="text"/>	
<input type="checkbox"/> Command AuthZ	<input type="text"/>	Name <input type="text"/>	

2. Authorization method configuration items

Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Default AuthZ	Configure the default authorization method and secondary authorization method for all types of users.
Name	Options include: <ul style="list-style-type: none">• Local—Performs local authorization.• None—All users are trusted and authorized. A user gets the corresponding default rights of the system.
Secondary Method	<ul style="list-style-type: none">• RADIUS—Performs RADIUS authorization. You must specify the RADIUS scheme to be used.• Not Set—Restore the default, that is, local authorization.
LAN-access AuthZ	Configure the authorization method and secondary authorization method for LAN access users.
Name	Options include: <ul style="list-style-type: none">• Local—Performs local authorization.• None—All users are trusted and authorized. A user gets the corresponding default rights of the system.
Secondary Method	<ul style="list-style-type: none">• RADIUS—Performs RADIUS authorization. You must specify the RADIUS scheme to be used.• Not Set—Uses the default authorization method.
Login AuthZ	Configure the authorization method and secondary authorization method for login users.
Name	Options include: <ul style="list-style-type: none">• Local—Performs local authorization.• None—All users are trusted and authorized. A user gets the corresponding default rights of the system.
Secondary Method	<ul style="list-style-type: none">• RADIUS—Performs RADIUS authorization. You must specify the RADIUS scheme to be used.
Name	<ul style="list-style-type: none">• Not Set—Uses the default authorization methods.

Return to [Configuration task list](#).

Configuring accounting methods for the ISP domain

Select **Authentication** → **AAA** from the navigation tree and then select the **Accounting** tab to enter the accounting method configuration page, as shown in [a](#).

a. Accounting method configuration page

Domain Setup	Authentication	Authorization	Accounting
--------------	----------------	---------------	------------

Accounting Configuration of AAA

Select an ISP domain:

<input type="checkbox"/> Accounting Optional	<input type="text" value="Disable"/>		
<input type="checkbox"/> Default Accounting	<input type="text" value="Local"/>	Name <input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> LAN-access Accounting	<input type="text"/>	Name <input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> Login Accounting	<input type="text"/>	Name <input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> PPP Accounting	<input type="text"/>	Name <input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> Portal Accounting	<input type="text"/>	Name <input type="text"/>	

2. Accounting method configuration items

Item	Description
Select an ISP domain	Select the ISP domain for which you want to specify authentication methods.
Accounting Optional	Specify whether to enable the accounting optional feature. When no accounting server is available or communication with the accounting servers fails, this feature allows users to use network resources and stops the switch from sending real-time accounting updates for the users.
Default Accounting	Configure the default accounting method and secondary accounting method for all types of users.
Name	Options include: <ul style="list-style-type: none"> Local—Performs local accounting. None—Performs no accounting.
Secondary Method	<ul style="list-style-type: none"> RADIUS—Performs RADIUS accounting. You must specify the RADIUS scheme to be used. Not Set—Restore the default, that is, local accounting.
LAN-access Accounting	Configure the accounting method and secondary accounting method for LAN access users.
Name	Options include: <ul style="list-style-type: none"> Local—Performs local accounting. None—Performs no accounting.
Secondary Method	<ul style="list-style-type: none"> RADIUS—Performs RADIUS accounting. You must specify the RADIUS scheme to be used. Not Set—Uses the default accounting methods.
Login Accounting	Configure the accounting method and secondary accounting method for login users.
Name	Options include: <ul style="list-style-type: none"> Local—Performs local accounting.

Item	Description
Secondary Method	<ul style="list-style-type: none"> None—Performs no accounting. RADIUS—Performs RADIUS accounting. You must specify the RADIUS scheme to be used. Not Set—Uses the default accounting methods.

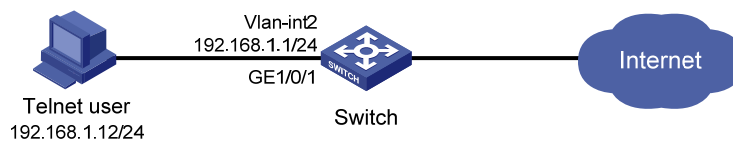
Return to [Configuration task list](#).

AAA configuration example

Network requirements

As shown in [a](#), configure the switch to perform local authentication, authorization, and accounting for Telnet users.

a. Network diagram for AAA configuration example



Configuration procedure

NOTE:

Enable the Telnet server function on the switch and configure the switch to use AAA for Telnet users. The configuration steps are omitted.

Configure IP addresses for the interfaces. (Omitted)

Configure a local user.

- Select **Device** → **Users** from the navigation tree and then select the **Create** tab, as shown in [a](#).

a. Configure a local user

Summary	Super Password	Create	Modify	Remove	Switch To Management
---------	----------------	---------------	--------	--------	----------------------

Create User			
Username	<input type="text" value="telnet"/> (1-55 Chars.)	Access Level	<input type="text" value="Management"/>
Password	<input type="password" value="abcd"/> (1-63 Chars.)	Confirm Password	<input type="password" value="abcd"/>
Password Display Mode	<input type="text" value="Simple"/>		
Service Type	<input type="checkbox"/> FTP Service <input checked="" type="checkbox"/> Telnet Service		

Summary

Username	Access Level	Service Type
admin	Management	Telnet

Note: Username cannot include characters " ", " ", ":", "|", "@", " ", "?", " ", "<" or ">".

- Enter **telnet** as the username.
- Select **Management** as the access level.
- Enter **abcd** as the password.
- Enter **abcd** to confirm the password.
- Select **Telnet Service** as the service type.
- Click **Apply**.

Configure ISP domain **test**.

- Select **Authentication** → **AAA** from the navigation tree. The domain configuration page appears, as shown in [b](#).

b. Configure ISP domain test

Domain Setup Authentication Authorization Accounting

ISP Domain

Domain Name test (1 - 24 Chars.)

Default Domain Disable

Apply

Please select the ISP domain(s)

Domain Name	Default Domain
system	Default

Select All Select None Remove

- Enter **test** as the domain name.
- Click **Apply**.

Configure the ISP domain to use local authentication.

- Select **Authentication** → **AAA** from the navigation tree and then select the **Authentication** tab, as shown in [c](#).

c. Configure the ISP domain to use local authentication

Domain Setup Authentication Authorization Accounting

Authentication Configuration of AAA

Select an ISP domain test

Default AuthN Local Name Secondary Method

LAN-access AuthN Name Secondary Method

Login AuthN Local Name Secondary Method

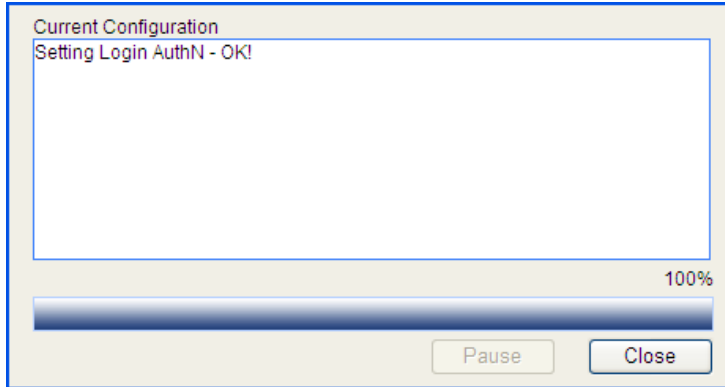
PPP AuthN Name Secondary Method

Portal AuthN Name

Apply

- Select the domain **test**.
- Select the **Login AuthN** check box and select the authentication method **Local**.
- Click **Apply**. A configuration progress dialog box appears, as shown in [d](#).

d. Configuration progress dialog box



- After the configuration process is complete, click **Close**.

Configure the ISP domain to use local authorization.

- Select **Authentication** → **AAA** from the navigation tree and then select the **Authorization** tab, as shown in e.

e. Configure the ISP domain to use local authorization

Domain Setup	Authentication	Authorization	Accounting
Authorization Configuration of AAA			
Select an ISP domain		test	
<input type="checkbox"/> Default AuthZ	Local	Name	Secondary Method
<input type="checkbox"/> LAN-access AuthZ		Name	Secondary Method
<input checked="" type="checkbox"/> Login AuthZ	Local	Name	Secondary Method
<input type="checkbox"/> PPP AuthZ		Name	Secondary Method
<input type="checkbox"/> Portal AuthZ		Name	
<input type="checkbox"/> Command AuthZ		Name	
<input type="button" value="Apply"/>			

- Select the domain **test**.
- Select the **Login AuthZ** check box and select the authorization method **Local**.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration progress is complete, click **Close**.

Configure the ISP domain to use local accounting.

- Select **Authentication** → **AAA** from the navigation tree and then select the **Accounting** tab, as shown in f.

f. Configure the ISP domain to use local accounting

Domain Setup	Authentication	Authorization	Accounting	
--------------	----------------	---------------	------------	--

Accounting Configuration of AAA

Select an ISP domain:

<input type="checkbox"/> Accounting Optional	<input type="text" value="Disable"/>			
<input type="checkbox"/> Default Accounting	<input type="text" value="Local"/>	Name	<input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> LAN-access Accounting	<input type="text"/>	Name	<input type="text"/>	Secondary Method <input type="text"/>
<input checked="" type="checkbox"/> Login Accounting	<input type="text" value="Local"/>	Name	<input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> PPP Accounting	<input type="text"/>	Name	<input type="text"/>	Secondary Method <input type="text"/>
<input type="checkbox"/> Portal Accounting	<input type="text"/>	Name	<input type="text"/>	

- Select the domain **test**.
- Select the **Login Accounting** check box and select the accounting method **Local**.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

Now, if you telnet to the switch and enter username **telnet@test** and password **abcd**, you should be serviced as a user in domain **test**.

RADIUS configuration

Introduction to RADIUS

The Remote Authentication Dial-In User Service (RADIUS) protocol implements Authentication, Authorization, and Accounting (AAA). For more information, see the chapter “AAA configuration”.

RADIUS uses the client/server model. It can protect networks against unauthorized access and is often used in network environments where both high security and remote user access are required. RADIUS defines the packet format and message transfer mechanism, and uses UDP as the transport layer protocol for encapsulating RADIUS packets. It uses UDP port 1812 for authentication and UDP port 1813 for accounting.

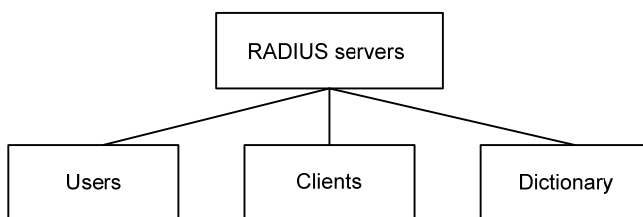
RADIUS was originally designed for dial-in user access. With the addition of new access methods, RADIUS has been extended to support additional access methods, for example, Ethernet and ADSL. RADIUS provides access authentication and authorization services, and its accounting function collects and records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

Client/server model

- Client—Generally, 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).
- Server—Generally, 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 the processing results (for example, rejecting or accepting the user access request) to the clients.

In general, the RADIUS server maintains the databases: Users, Clients, and Dictionary, as shown in [a](#).

a. RADIUS server components



- Users—Stores user information such as the usernames, passwords, applied protocols, and IP addresses.
- Clients—Stores information about RADIUS clients, such as the 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 the information exchange security. In addition,

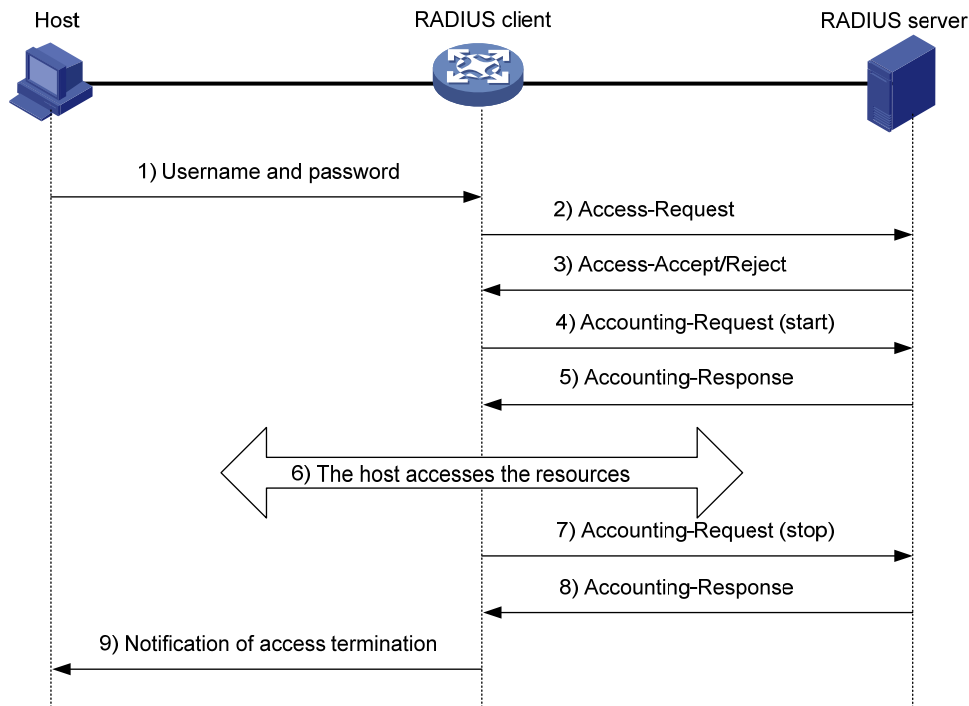
to prevent user passwords from being intercepted on insecure networks, RADIUS encrypts passwords before transmitting them.

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

Basic message exchange process of RADIUS

a illustrates the interaction of the host, the RADIUS client, and the RADIUS server.

a. Basic message exchange process of RADIUS



RADIUS operates in the following manner:

Table 122 The host initiates a connection request that carries the user's username and password to the RADIUS client.

Table 123 After receiving 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.

Table 124 The RADIUS server authenticates the username and password. If the authentication succeeds, the server sends back an Access-Accept message containing the user's authorization information. If the authentication fails, the server returns an Access-Reject message.

Table 125 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.

Table 126 The RADIUS server returns a start-accounting response (Accounting-Response) and starts accounting.

Table 127 The user accesses the network resources.

Table 128 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.

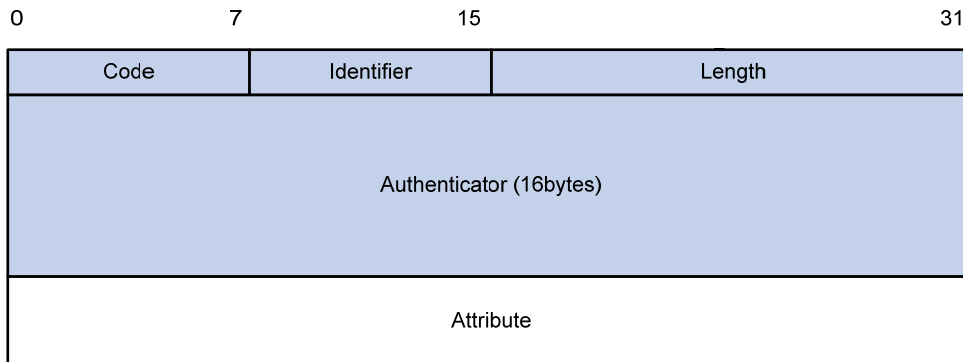
Table 129 The RADIUS server returns a stop-accounting response (Accounting-Response) and stops accounting for the user.

Table 130 The user stops access to network resources.

RADIUS packet format

RADIUS uses UDP to transmit messages. It ensures the smooth message exchange between the RADIUS server and the client through a series of mechanisms, including the timer management mechanism, retransmission mechanism, and slave server mechanism.

a. RADIUS packet format



Descriptions of the fields are as follows:

Table 131 The Code field (1-byte long) indicates the type of the RADIUS packet.

2. 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, that is, the authentication succeeds, 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 server rejects the user and 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/stop accounting for the user. It contains the Acct-Status-Type attribute, which indicates whether the server is requested to start the accounting or to end the accounting.
5	Accounting-Response	From the server to the client. The server sends to the client a packet of this type to notify that it has received the Accounting-Request and has correctly started recording the accounting information.

Table 132 The Identifier field (1 byte long) is used to match request packets and response packets and to detect duplicate request packets. Request and response packets of the same type have the same identifier.

Table 133 The Length field (2 byte 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.

Table 134 The Authenticator field (16 byte 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.

Table 135 The Attributes field, variable in length, carries the specific authentication, authorization, and accounting information that defines the configuration details of the request or response. This field may contain multiple attributes, each with three sub-fields: Type, Length, and Value.

- Type (1 byte long)—Indicates the type of the attribute. It is in the range 1 to 255. Commonly used attributes for RADIUS authentication, authorization and accounting are listed in 3.
- 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.

3. 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

No.	Attribute	No.	Attribute
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
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

NOTE:

The attribute types listed in 3 are defined by RFC 2865, RFC 2866, RFC 2867, and RFC 2868.

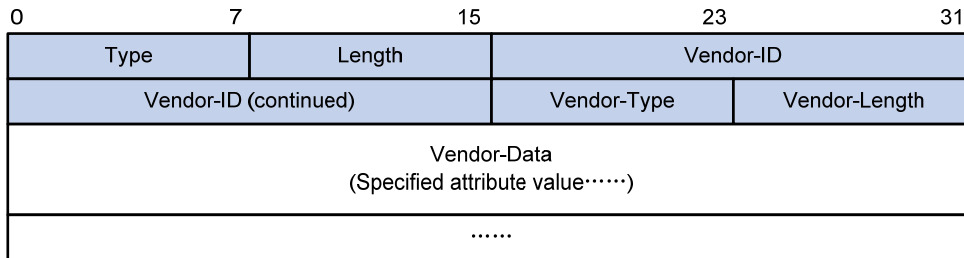
Extended RADIUS attributes

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

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

- Vendor-ID—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.
- 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.

a. Segment of a RADIUS packet containing an extended attribute



Protocols and standards

- RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*
- RFC 2866, *RADIUS Accounting*
- RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*
- RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*
- RFC 2869, *RADIUS Extensions*

Configuring RADIUS

Configuration task list

NOTE:

The RADIUS scheme configured through the web interface is named **system**.

If there is no RADIUS scheme named **system** in the system, when you select **Authentication** → **RADIUS** to enter the RADIUS module, a scheme named **system** is created automatically.

1. RADIUS configuration task list

Task	Description	
Configuring RADIUS authentication servers	<p>Required</p> <p>Configure the information related to the primary and secondary RADIUS authentication servers.</p> <p>By default, no RADIUS authentication server is configured.</p>	<p>For more information, see "Configuring RADIUS servers."</p>

Task	Description
Configuring RADIUS accounting servers	Optional Configure the information related to the primary and secondary RADIUS accounting servers. By default, no RADIUS accounting server is configured.
Configuring RADIUS parameters	Required Configure the parameters that are necessary for information exchange between the device and RADIUS servers.

Configuring RADIUS servers

From the navigation tree, select **Authentication** → **RADIUS**. The RADIUS server configuration page appears, as shown in a.

a. RADIUS server configuration

RADIUS Server	RADIUS Setup
Server Type:	Authentication Server ▼
Primary Server IP:	0.0.0.0 *
Primary Server UDP Port:	1812 *(1-65535)
Primary Server Status:	block ▼
Secondary Server IP:	0.0.0.0 *
Secondary Server UDP Port:	1812 *(1-65535)
Secondary Server Status:	block ▼

Items marked with an asterisk(*) are required

Apply

2. RADIUS server configuration

Item	Description
Server Type	Specify the type of the server to be configured, which can be Authentication Server and Accounting Sever.
Primary Server IP	Specify the IP address of the primary server. If no primary server is specified, the text box displays 0.0.0.0. To remove the previously configured primary server, enter 0.0.0.0 in the text box. The specified IP address of the primary server cannot be the same as that of the secondary server.
Primary Server UDP Port	Specify the UDP port of the primary server. If the IP address of the primary server is not specified or the specified IP address is to be removed, the port number is 1812 for authentication or 1813 for accounting.

Item	Description
Primary Server Status	<p>Set the status of the primary server, including:</p> <ul style="list-style-type: none"> • active: The server is working normally. • blocked: The server is down. <p>If the IP address of the primary server is not specified or the specified IP address is to be removed, the status is blocked.</p>
Secondary Server IP	<p>Specify the IP address of the secondary server.</p> <p>If no secondary server is specified, the text box displays 0.0.0.0.</p> <p>To remove the previously configured secondary server, enter 0.0.0.0 in the text box.</p> <p>The specified IP address of the secondary server cannot be the same as that of the primary server.</p>
Secondary Server UDP Port	<p>Specify the UDP port of the secondary server.</p> <p>If the IP address of the secondary server is not specified or the specified IP address is to be removed, the port number is 1812 for authentication or 1813 for accounting.</p>
Secondary Server Status	<p>Status of the secondary server, including:</p> <ul style="list-style-type: none"> • active: The server is working normally. • blocked: The server is down. <p>If the IP address of the secondary server is not specified or the specified IP address is to be removed, the status is blocked.</p>

Return to [RADIUS configuration task list](#).

Configuring RADIUS parameters

From the navigation tree, select **Authentication** → **RADIUS** and then select the **RADIUS Setup** tab to enter the RADIUS parameter configuration page, as shown in [a](#).

a. RADIUS parameter configuration

RADIUS Server	RADIUS Setup
Server Type:	standard <input type="button" value="v"/>
<input type="checkbox"/> Authentication Server Shared Key:	<input type="text"/> (1-64 Chars.)
Confirm Authentication Shared Key:	<input type="text"/>
<input type="checkbox"/> Accounting Server Shared Key:	<input type="text"/> (1-64 Chars.)
Confirm Accounting Shared Key:	<input type="text"/>
NAS-IP:	<input type="text"/>
Timeout Interval:	3 <input type="button" value="*seconds(1-10)"/>
Timeout Retransmission Times:	3 <input type="button" value="*(1-20)"/>
Realtime-Accounting Interval:	12 <input type="button" value="*minutes(0-60, Must be a multiple of 3)"/>
Realtime-Accounting Packet Retransmission Times:	5 <input type="button" value="*(1-255)"/>
Stop-Accounting Buffer:	enable <input type="button" value="v"/>
Stop-Accounting Packet Retransmission Times:	500 <input type="button" value="*(10-65535)"/>
Quiet Interval:	5 <input type="button" value="*minutes(1-255)"/>
Username Format:	with-domain <input type="button" value="v"/>
Unit of Data Flows:	byte <input type="button" value="v"/>
Unit of Packets:	packet <input type="button" value="v"/>

Items marked with an asterisk(*) are required

2. RADIUS parameters

Item	Description
Server Type	<p>Specify the type of the RADIUS server supported by the device, including:</p> <ul style="list-style-type: none"> extended: Specifies an extended RADIUS server (usually a CAMS or iMC server). That is, the RADIUS client and RADIUS server communicate using the proprietary RADIUS protocol and packet format. standard: Specifies a standard RADIUS server. That is, the RADIUS client and RADIUS server communicate using the standard RADIUS protocol and packet format defined in RFC 2138/2139 or later.
Authentication Server Shared Key	Specify and confirm the shared key for the authentication server. These two parameters must have the same values.
Confirm Authentication Shared Key	
Accounting Server Shared Key	Specify and confirm the shared key for the accounting server. These two parameters must have the same values.
Confirm Accounting Shared Key	
NAS-IP	Specify the source IP address for the device to use in RADIUS packets to be sent to the RADIUS server. It is recommended to use a loopback interface address instead of a physical interface address as the source IP address, because if the physical interface is down, the response packets from the server cannot reach the device.
Timeout Interval	Set the RADIUS server response timeout.

Item	Description
Timeout Retransmission Times	<p>Set the maximum number of transmission attempts.</p> <p>The product of the timeout value and the number of retransmission attempts cannot exceed 75.</p>
Realtime-Accounting Interval	<p>Set the real-time accounting interval, whose value must be n times 3 (n is an integer).</p> <p>To implement real-time accounting on users, it is necessary to set the real-time accounting interval. After this parameter is specified, the device will send the accounting information of online users to the RADIUS server every the specified interval.</p> <p>The value of the real-time accounting interval is related to the requirement on the performance of the NAS and RADIUS server. The smaller the value, the higher the requirement. It is recommended to set a large value if the number of users is equal to or larger than 1000. 3 shows the relationship between the interval value and the number of users.</p>
Realtime-Accounting Packet Retransmission Times	<p>Set the maximum number of real-time accounting request retransmission times.</p>
Stop-Accounting Buffer	<p>Enable or disable buffering stop-accounting requests without responses in the device.</p>
Stop-Accounting Packet Retransmission Times	<p>Set the maximum number of transmission attempts if no response is received for the stop-accounting packet.</p>
Quiet Interval	<p>Specify the interval the primary server has to wait before being active</p>
Username Format	<p>Set the format of username sent to the RADIUS server.</p> <p>A username is generally in the format of userid@isp-name, of which isp-name is used by the device to determine the ISP domain to which a user belongs. If a RADIUS server does not accept a username including an ISP domain name, you can configure the device to remove the domain name of a username before sending it to the RADIUS server.</p> <p>without-domain: Specifies to remove the domain name of a username that is to be sent to the RADIUS server.</p> <p>with-domain: Specifies to keep the domain name of a username that is to be sent to the RADIUS server.</p>
Unit of Data Flows	<p>Specify the unit for data flows sent to the RADIUS server, which can be:</p> <ul style="list-style-type: none"> • byte • kilo-byte • mega-byte • giga-byte

Item	Description
Unit of Packets	Specify the unit for data packets sent to the RADIUS server, which can be <ul style="list-style-type: none"> • one-packet • kilo-packet • mega-packet • giga-packet

3. Relationship between the real-time accounting interval and the number of users

Number of users	Real-time accounting interval (in minutes)
1 to 99	3
100 to 499	6
500 to 999	12
f1000	f15

Return to [RADIUS configuration task list](#).

RADIUS configuration example

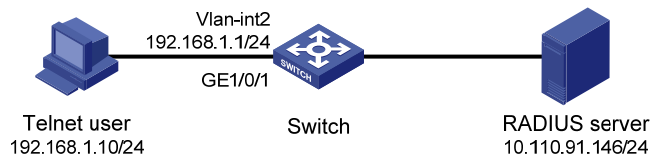
Network requirements

As shown in [a](#), configure the switch to let the RADIUS server authenticate and keep accounts on the user (record the online duration of the Telnet user).

On the RADIUS server (a CAMS or iMC server, using the default port for authentication and accounting), the Telnet user's username and password and the shared key **expert** have been configured for packet exchange with the switch.

On the switch, it is required to configure the shared key for packet exchange with the RADIUS server as **expert**, and configure the system to remove the domain name of a username before sending it to the RADIUS server.

a. Network diagram for RADIUS server configuration



Configuration procedure

NOTE:

Enable the Telnet server function, and configure the switch to use AAA for authentication, authorization and accounting of Telnet users. Detailed configuration steps are omitted here.

Table 136 Configure IP addresses for the interfaces. Detailed configuration steps are omitted here.

Table 137 Configure RADIUS scheme **system**

Configure the RADIUS authentication server.

- From the navigation tree, select **Authentication** → **RADIUS**. The RADIUS server configuration page appears.

b. Configure the RADIUS authentication server

RADIUS Server	RADIUS Setup
Server Type:	Authentication Server <input type="button" value="v"/>
Primary Server IP:	10.110.91.146 *
Primary Server UDP Port:	1812 *(1-65535)
Primary Server Status:	active <input type="button" value="v"/>
Secondary Server IP:	0.0.0.0 *
Secondary Server UDP Port:	1812 *(1-65535)
Secondary Server Status:	block <input type="button" value="v"/>

Items marked with an asterisk(*) are required

- Select **Authentication Server** as the server type.
- Enter **10.110.91.146** as the IP address of the primary authentication server
- Enter **1812** as the UDP port of the primary authentication server.
- Select **active** as the primary server status.
- Click **Apply**.

Configure the RADIUS accounting server.

c. Configure the RADIUS accounting server

RADIUS Server	RADIUS Setup
Server Type:	Accounting Server <input type="button" value="v"/>
Primary Server IP:	10.110.91.146 *
Primary Server UDP Port:	1813 *(1-65535)
Primary Server Status:	active <input type="button" value="v"/>
Secondary Server IP:	0.0.0.0 *
Secondary Server UDP Port:	1813 *(1-65535)
Secondary Server Status:	block <input type="button" value="v"/>

Items marked with an asterisk(*) are required

- Select **Accounting Server** as the server type.
- Enter **10.110.91.146** as the IP address of the primary accounting server.
- Enter **1813** as the UDP port of the primary accounting server.

- Select **active** as the primary server status.
- Click **Apply**.

Configure the parameters for communication between the switch and the RADIUS servers.

- Select the **RADIUS Setup** tab.

d. Configure RADIUS parameters

RADIUS Server RADIUS Setup

Server Type: extended

Authentication Server Shared Key: (1-64 Chars.)

Confirm Authentication Shared Key:

Accounting Server Shared Key: (1-64 Chars.)

Confirm Accounting Shared Key:

NAS-IP:

Timeout Interval: 3 seconds(1-10)

Timeout Retransmission Times: 3 *(1-20)

Realtime-Accounting Interval: 12 minutes(0-60, Must be a multiple of 3)

Realtime-Accounting Packet Retransmission Times: 5 *(1-255)

Stop-Accounting Buffer: enable

Stop-Accounting Packet Retransmission Times: 500 *(10-65535)

Quiet Interval: 5 minutes(1-255)

Username Format: without-domain

Unit of Data Flows: byte

Unit of Packets: packet

Items marked with an asterisk(*) are required

Apply

- Select **extended** as the server type.
- Select the **Authentication Server Shared Key** check box and enter **expert** in the text box.
- Enter **expert** in the **Confirm Authentication Shared Key** text box.
- Select the **Accounting Server Shared Key** check box and enter **expert** in the text box.
- Enter **expert** in the **Confirm Accounting Shared Key** text box.
- Select **without-domain** for **Username Format**.
- Click **Apply**

Table 138 Configure AAA

Create an ISP domain.

- From the navigation tree, select **Authentication** → **AAA**. The domain setup page appears.

e. Create an ISP domain

Domain Setup Authentication Authorization Accounting

ISP Domain

Domain Name test (1 - 24 Chars.)

Default Domain Enable

Apply

Please select the ISP domain(s)

Domain Name	Default Domain
system	Default

Select All Select None Remove

- Enter **test** in the **Domain Name** textbox.
- Select **Enable** to use the domain as the default domain.
- Click **Apply**.

Configure the AAA authentication method for the ISP domain.

- Select the **Authentication** tab.

f. Configure the AAA authentication method for the ISP domain

Domain Setup Authentication Authorization Accounting

Authentication Configuration of AAA

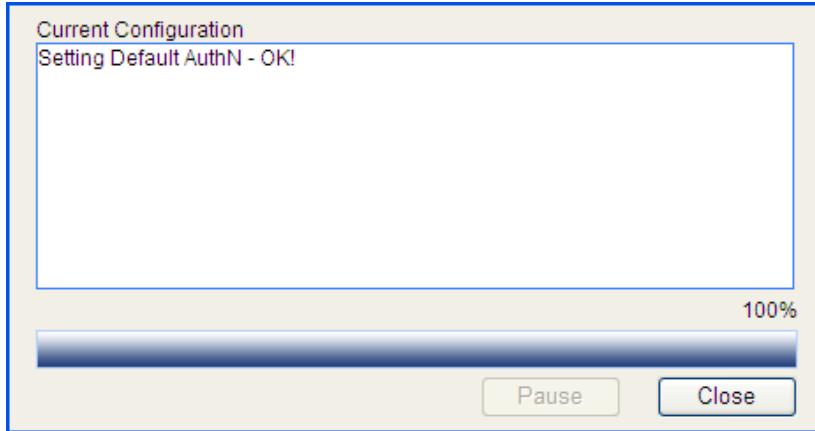
Select an ISP domain test

<input checked="" type="checkbox"/> Default AuthN	RADIUS	Name system	Secondary Method
<input type="checkbox"/> LAN-access AuthN		Name	Secondary Method
<input type="checkbox"/> Login AuthN		Name	Secondary Method
<input type="checkbox"/> PPP AuthN		Name	Secondary Method
<input type="checkbox"/> Portal AuthN		Name	Secondary Method

Apply

- Select the domain name **test**.
- Select the **Default AuthN** checkbox and then select **RADIUS** as the authentication mode.
- Select **system** from the **Name** drop-down list to use it as the authentication scheme.
- Click **Apply**. A configuration progress dialog box appears, as shown in [g](#).

g. Configuration progress dialog box



- After the configuration process is complete, click **Close**.

Configure the AAA authorization method for the ISP domain.

- Select the **Authorization** tab.

h. Configure the AAA authorization method for the ISP domain

Domain Setup	Authentication	Authorization	Accounting
--------------	----------------	---------------	------------

Authorization Configuration of AAA

Select an ISP domain	test			
<input checked="" type="checkbox"/> Default AuthZ	RADIUS	Name	system	Secondary Method
<input type="checkbox"/> LAN-access AuthZ		Name		Secondary Method
<input type="checkbox"/> Login AuthZ		Name		Secondary Method
<input type="checkbox"/> PPP AuthZ		Name		Secondary Method
<input type="checkbox"/> Portal AuthZ		Name		
<input type="checkbox"/> Command AuthZ		Name		

Apply

- Select the domain name **test**.
- Select the **Default AuthZ** checkbox and then select **RADIUS** as the authorization mode.
- Select **system** from the **Name** drop-down list to use it as the authorization scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

Configure the AAA accounting method for the ISP domain, and enable accounting optional.

- Select the **Accounting** tab.

i. Configure the AAA accounting method for the ISP domain

Domain Setup	Authentication	Authorization	Accounting	
--------------	----------------	---------------	------------	--

Accounting Configuration of AAA

Select an ISP domain	test		
<input checked="" type="checkbox"/> Accounting Optional	Enable		
<input checked="" type="checkbox"/> Default Accounting	RADIUS	Name system	Secondary Method
<input type="checkbox"/> LAN-access Accounting		Name	Secondary Method
<input type="checkbox"/> Login Accounting		Name	Secondary Method
<input type="checkbox"/> PPP Accounting		Name	Secondary Method
<input type="checkbox"/> Portal Accounting		Name	Secondary Method

Apply

- Select the domain name **test**.
- Select the **Accounting Optional** checkbox and then select **Enable**.
- Select the **Default Accounting** checkbox and then select **RADIUS** as the accounting mode.
- Select **system** from the **Name** drop-down list to use it as the accounting scheme.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close**.

Configuration guidelines

When you configure the RADIUS client, note the following guidelines:

- When you modify the parameters of the RADIUS scheme, the system does not check whether the scheme is being used by users.
- After accounting starts, update-accounting and stop-accounting packets will be sent to the designated server, and no primary/secondary server switchover will take place even if the designated server fails. Such a switchover can take place only during AAA session establishment.
- If an AAA server has active TCP connections, it cannot be removed.
- RADIUS does not support accounting for FTP users.
- If the CAMS/iMC server is used as the RADIUS server, it is necessary to configure accounting as optional for users in the ISP domain because the CAMS/iMC server does not respond to accounting packets.

Users

This module allows you to configure local users and user groups.

Local user

A local user represents a set of user attributes configured on a device (such as the user password, service type, and authorization attribute), and is uniquely identified by the username. For a user requesting a network service to pass local authentication, you must add an entry as required in the local user database of the device. For more information about local authentication, see the chapter “AAA configuration”.

User group

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 management of user attributes for the local users in the group. All local users in a user group inherit the user attributes of the group, but if you configure user attributes for a local user, the settings of the local user take precedence over the settings for the user group.

By default, every newly added local user belongs to a user group named system, which is automatically created by the system.

Configuring users

Configuring a local user

Select **Authentication** → **Users** from the navigation tree. The **Local User** page appears, displaying all local users, as shown in a. Click **Add** to enter the local user configuration page.

a. Local user list

Local User User Group

▶ Search Item: User Name Keywords: Search

User Name	Service Type	Level	VLAN	ACL	User Profile	User Group	Expire Time	Operation
admin	Telnet	Management				system		

Add

b. Local user configuration page

Local User	User Group
------------	------------

Add Local User

Username: *(1-55)

Password: (1-63)

Confirm: (1-63)

Group: ▼

Service-type: FTP Telnet LAN-Access SSH

Expire-time: (From 2000 to 2035, HH:MM:SS-YYYY/MM/DD)

Level: ▼

VLAN: (1-4094)

ACL: (2000-4999)

User-profile: (1-32)

Items marked with an asterisk(*) are required

2. Local user configuration items

Item	Description
Username	Specify a name for the local user.
Password	Specify and confirm the password of the local user. The settings of these two fields must be the same.
Confirm	
Group	Select a user group for the local user. For more information about user group configuration, see “Configuring a user group.”
Service-type	Select the service types for the local user to use, including FTP, Telnet, LAN access (accessing through the Ethernet, such as 802.1x users), and SSH. ⚠ IMPORTANT: If you do not specify any service type for a local user who uses local authentication, the user cannot pass authentication and therefore cannot log in.
Expire-time	Specify an expiration time for the local user, in the format HH:MM:SS-YYYY/MM/DD. When authenticating a local user with the expiration time argument configured, the access device checks whether the expiration time has elapsed. If not, the device permits the user to log in.
Level	Select an authorization level for the local user, which can be Visitor, Monitor, Configure, or Management, in ascending order of priority. ⚠ IMPORTANT: Every authorization attribute

Item	Description	
VLAN	Specify the VLAN to be authorized to the local user after the user passes authentication.	has its definite application environments and purposes. When configuring authorization attributes for a local user, determine what attributes are needed first.
ACL	Specify the ACL to be used by the access device to restrict the access of the local user after the user passes authentication.	
User-profile	Specify the user profile for the local user. NOTE: HP V1910 Switch Series does not support user-profile configuration.	



Configuring a user group

Select **Authentication** → **Users** from the navigation tree, and then select the **User Group** tab to display the existing user groups, as shown in **a**. Then, click **Add** to enter the user group configuration page, as shown in **b**.

a. User group list

Local User **User Group**

▶ Search Item: Group Name ▼ Keywords: Search

Group Name	Level	VLAN	ACL	User Profile	Operation
system	Vistor				 

Add

b. User group configuration page

Local User **User Group**

Add User Group

Group-name: *(1-32)

Level: ▼

VLAN: (1-4094)

ACL: (2000-4999)

User-profile (1-32)

Items marked with an asterisk(*) are required

Apply **Cancel**

2. User group configuration items

Item	Description
Group-name	Specify a name for the user group.
Level	Select an authorization level for the user group, which can be Visitor, Monitor, Configure, or Management, in ascending order of priority.
VLAN	Specify the VLAN to be authorized to users of the user group after the users pass authentication.
ACL	Specify the ACL to be used by the access device to control the access of users of the user group after the users pass authentication.
User-profile	Specify the user profile for the user group. NOTE: HP V1910 Switch Series does not support user-profile configuration.

PKI configuration

PKI overview

The Public Key Infrastructure (PKI) is a hierarchical framework designed for providing information security through public key technologies and digital certificates and verifying the identities of the digital certificate owners.

PKI employs digital certificates, which are bindings of certificate owner identity information and public keys. It allows users to obtain certificates, use certificates, and revoke certificates. By leveraging digital certificates and relevant services like certificate distribution and blacklist publication, PKI supports authenticating the entities involved in communication, and thus guaranteeing the confidentiality, integrity and non-repudiation of data.

PKI terms

Digital certificate

A digital certificate is a file signed by a certificate authority (CA) that contains a public key and the related user identity information. A simplest digital certificate contains a public key, an entity name, and a digital signature from the CA. Generally, a digital certificate also includes the validity period of the key, the name of the CA and the sequence number of the certificate. A digital certificate must comply with the international standard of ITU-T_X.509. This document involves local certificate and CA certificate. A local certificate is a digital certificate signed by a CA for an entity. A CA certificate, also known as a “root certificate”, is signed by the CA for itself.

CRL

An existing certificate may need to be revoked when, for example, the user name changes, the private key leaks, or the user stops the business. Revoking a certificate is to remove 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.

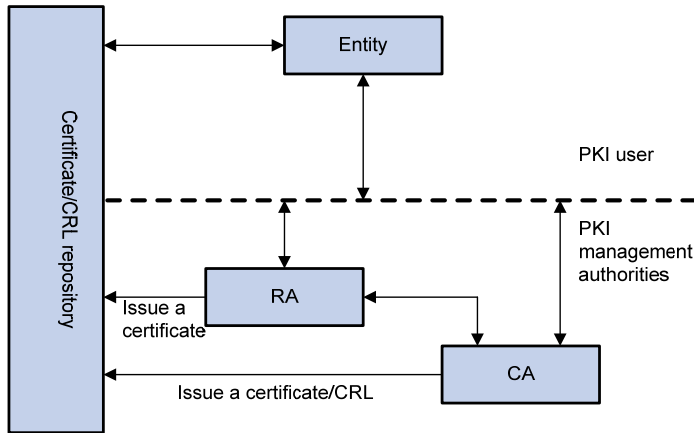
CA policy

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 may 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.

Architecture of PKI

A PKI system consists of entities, a CA, a registration authority (RA) and a PKI repository, as shown in [a](#).

a. 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 certificate authority (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. It only examines the qualifications of users; it does not sign certificates. Sometimes, a CA assumes the registration management responsibility and no independent RA exists. The PKI standard recommends that an independent RA be used for registration management to achieve higher security of application systems.

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, and it provides a simple query function.

LDAP is a protocol for accessing and managing PKI information. An LDAP server stores user information and digital certificates from the RA server and provides directory navigation service. From an LDAP server, an entity can retrieve digital certificates of its own and other entities.

Applications of PKI

The PKI technology can satisfy the security requirements of online transactions. As an infrastructure, PKI has a wide range of applications. Here are some application examples.

VPN

A virtual private network (VPN) is a private data communication network built on the public communication infrastructure. A VPN can leverage network layer security protocols (for instance, IPSec) in conjunction with PKI-based encryption and digital signature technologies to achieve confidentiality.

Secure email

Emails require confidentiality, integrity, authentication, and non-repudiation. PKI can address these needs. The secure e-mail 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 a Secure Sockets Layer (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 the communication parties can verify the identity of each other through digital certificates.

Operation of PKI

In a PKI-enabled network, an entity can request a local certificate from the CA and the device can check the validity of certificate. The following describes how it works:

Table 139 An entity submits a certificate request to the CA.

Table 140 The RA verifies the identity of the entity and then sends the identity information and the public key with a digital signature to the CA.

Table 141 The CA verifies the digital signature, approves the application, and issues a certificate.

Table 142 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.

Table 143 The entity retrieves the certificate. With the certificate, the entity can communicate with other entities safely through encryption and digital signature.

Table 144 The entity makes a request to the CA when it needs to revoke its certificate. The CA approves the request, updates the CRLs and publishes the CRLs on the LDAP server.

Configuring PKI

Configuration task list

The device supports the following PKI certificate request modes:

- **Manual**—In manual mode, you need to retrieve a CA certificate, generate a local RSA key pair, and submit a local certificate request for an entity.
- **Auto**—In auto mode, an entity automatically requests a certificate through the Simple Certification Enrollment Protocol (SCEP) when it has no local certificate or the present certificate is about to expire.

You can specify the PKI certificate request mode for a PKI domain. Different PKI certificate request modes require different configurations:

Requesting a certificate manually

Perform the tasks in 1 to request a certificate manually.

1. Configuration task list for requesting a certificate manually

Task	Remarks
Creating a PKI entity	<p>Required</p> <p>Create a PKI entity and configure the identity information.</p> <p>A certificate is the binding of a public key and an entity, where an entity is the collection of the identity information of a user. A CA identifies a certificate applicant by entity.</p> <p>! IMPORTANT:</p> <p>The identity settings of an entity must be compliant to the CA certificate issue policy. Otherwise, the certificate request may be rejected.</p>
Creating a PKI domain	<p>Required</p> <p>Create a PKI domain, setting the certificate request mode to Manual.</p> <p>Before requesting a PKI certificate, an entity needs to be configured with some enrollment information, which is referred to as a PKI domain.</p> <p>A PKI domain is intended only for convenience of reference by other applications like SSL, and has only local significance.</p>
Generating an RSA key pair	<p>Required</p> <p>Generate a local RSA key pair.</p> <p>By default, no local RSA key pair exists.</p> <p>Generating an RSA key pair is an important step in certificate request. The key pair includes a public key and a private key. The private key is kept by the user, and the public key is transferred to the CA along with some other information.</p> <p>! IMPORTANT:</p> <p>If a local certificate already exists, you must remove the certificate before generating a new key pair, so as to keep the consistency between the key pair and the local certificate.</p>
Retrieving a certificate	<p>Required</p> <p>Certificate retrieval serves two purposes:</p> <ul style="list-style-type: none">• Locally store the certificates associated with the local security domain for improved query efficiency and reduced query count,• Prepare for certificate verification. <p>! IMPORTANT:</p> <p>If a local CA certificate already exists, you cannot perform the CA certificate retrieval operation. This will avoid possible mismatch between certificates and registration information resulting from relevant changes. To retrieve the CA certificate, you need to remove the CA certificate and local certificate first.</p>

Task	Remarks
Requesting a local certificate	<p>Required</p> <p>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.</p> <p>A certificate request can be submitted to a CA in two ways: online and offline.</p> <ul style="list-style-type: none"> In online mode, if the request is granted, the local certificate will be retrieved to the local system automatically. In offline mode, you need to retrieve the local certificate by an out-of-band means. <p>! IMPORTANT:</p> <p>If a local certificate already exists, you cannot perform the local certificate retrieval operation. This is to avoid possible mismatch between the local certificate and registration information resulting from relevant changes. To retrieve a new local certificate, you need to remove the CA certificate and local certificate first.</p>
Destroying the RSA key pair	<p>Optional</p> <p>Destroy the existing RSA key pair and the corresponding local certificate.</p> <p>If the certificate to be retrieved contains an RSA key pair, you need to destroy the existing key pair. Otherwise, the retrieving operation will fail.</p>
Retrieving a certificate	<p>Optional</p> <p>Retrieve an existing certificate.</p>
Retrieving and displaying a CRL	<p>Optional</p> <p>Retrieve a CRL and display its contents.</p>

Requesting a Certificate Automatically

Perform the tasks in 1 to configure the PKI system to request a certificate automatically.

1. Configuration task list for requesting a certificate automatically



Task	Remarks
Creating a PKI entity	<p>Required</p> <p>Create a PKI entity and configure the identity information.</p> <p>A certificate is the binding of a public key and an entity, where an entity is the collection of the identity information of a user. A CA identifies a certificate applicant by entity.</p> <p>The identity settings of an entity must be compliant to the CA certificate issue policy. Otherwise, the certificate request may be rejected.</p>
Creating a PKI domain	<p>Required</p> <p>Create a PKI domain, setting the certificate request mode to Auto.</p> <p>Before requesting a PKI certificate, an entity needs to be configured with some enrollment information, which is referred to as a PKI domain.</p> <p>A PKI domain is intended only for convenience of reference by other applications like SSL, and has only local significance.</p>

Task	Remarks
Destroying the RSA key pair	Optional Destroy the existing RSA key pair and the corresponding local certificate. If the certificate to be retrieved contains an RSA key pair, you need to destroy the existing key pair. Otherwise, the retrieving operation will fail.
Retrieving a certificate	Optional Retrieve an existing certificate.
Retrieving and displaying a CRL	Optional Retrieve a CRL and display its contents.

Creating a PKI entity

Select **Authentication** → **PKI** from the navigation tree. The PKI entity list page is displayed by default, as shown in **a**. Click **Add** on the page to enter the PKI entity configuration page, as shown in **b**.

a. PKI entity list

Entity	Domain	Certificate	CRL						
entity1	aaa							1.1.1.10	 

b. PKI entity configuration page

Entity	Domain	Certificate	CRL						
Add PKI Entity									
Entity Name:	<input type="text"/>	* (1-15 Chars.)							
Common Name:	<input type="text"/>	* (1-31 Chars.)							
IP Address:	<input type="text"/>								
FQDN:	<input type="text"/>	(1-127 Chars.)							
Country/Region Code:	<input type="text"/>	(Country/Region name symbol, two characters compliant to ISO 3166 standard.)							
State:	<input type="text"/>	(1-31 Chars.)							
Locality:	<input type="text"/>	(1-31 Chars.)							
Organization:	<input type="text"/>	(1-31 Chars.)							
Organization Unit:	<input type="text"/>	(1-31 Chars.)							
Items marked with an asterisk(*) are required									
<input type="button" value="Apply"/>					<input type="button" value="Cancel"/>				

2. PKI entity configuration items

Item	Description
Entity Name	Type the name for the PKI entity.
Common Name	Type the common name for the entity.
IP Address	Type the IP address of the entity.
FQDN	Type the fully qualified domain name (FQDN) for the entity. An FQDN is 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 indicates the host name and whatever.com the domain name.
Country/Region Code	Type the country or region code for the entity.
State	Type the state or province for the entity.
Locality	Type the locality for the entity.
Organization	Type the organization name for the entity.
Organization Unit	Type the unit name for the entity.


Return to [Configuration task list for requesting a certificate manually](#).

Return to [Configuration task list for requesting a certificate automatically](#).

Creating a PKI domain

Select **Authentication** → **PKI** from the navigation tree, and then select the **Domain** tab to enter the page displaying existing PKI domains, as shown in [a](#). Then, click **Add** to enter the PKI domain configuration page, and click **Display Advanced Config** to display the advanced configuration items, as shown in [b](#).

a. PKI domain list

Entity	Domain	Certificate	CRL		
	Domain Name	CA Identifier	Entity Name	Request Mode	Operation
	abcd		entity1	Manual	 
<input type="button" value="Add"/>					

b. PKI domain configuration page

Entity	Domain	Certificate	CRL
--------	--------	-------------	-----

Add PKI Domain

Domain Name: * (1-15 Chars.)

CA Identifier: (1-63 Chars.)

Entity Name:

Institution:

Requesting URL: (1-127 Chars.)

LDAP IP: Port: Version:

Request Mode:

Hash:

Fingerprint: (32 Hex)

Polling Count: (1-100, Default = 50)

Polling Interval: minutes(5-168, Default = 20)

Enable CRL Checking

CRL Update Period: hours(1-720)

CRL URL: (1-127 Chars.)

Items marked with an asterisk(*) are required

2. PKI domain configuration items

Item	Description
Domain Name	Type the name for the PKI domain.
CA Identifier	Type the identifier of the trusted CA. An entity requests a certificate from a trusted CA. The trusted CA takes the responsibility of certificate registration, distribution, and revocation, and query. In offline mode, this item is optional; while in other modes, this item is required.
Entity Name	Select the local PKI entity. When submitting a certificate request to a CA, an entity needs to show its identity information. Available PKI entities are those that have been configured.
Institution	Select the authority for certificate request. <ul style="list-style-type: none"> CA: Indicates that the entity requests a certificate from a CA. RA: Indicates that the entity requests a certificate from an RA. RA is recommended.

Item	Description
Requesting URL	<p>Type the URL of the RA.</p> <p>The entity will submit the certificate request to the server at this URL through the SCEP protocol. The SCEP protocol is intended for communication between an entity and an authentication authority.</p> <p>In offline mode, this item is optional; while in other modes, this item is required.</p> <p>! IMPORTANT:</p> <p>This item does not support domain name resolution.</p>
LDAP IP	Type the IP address, port number and version of the LDAP server.
Port	In a PKI system, the storage of certificates and CRLs is a crucial problem, which is usually addressed by deploying an LDAP server.
Version	
Request Mode	Select the online certificate request mode, which can be auto or manual.
Password Encrypt	<p>Select this check box to display the password in cipher text.</p> <p>This check box is available only when the certificate request mode is set to Auto.</p>
Password	<p>Type the password for certificate revocation.</p> <p>This item is available only when the certificate request mode is set to Auto.</p>
Hash	<p>Specify the hash algorithm and fingerprint for verification of the CA root certificate.</p> <p>Upon receiving the root certificate of the CA, an entity needs to verify the fingerprint of the root certificate, namely, the hash value of the root certificate content. This hash value is unique to every certificate. If the fingerprint of the root certificate does not match the one configured for the PKI domain, the entity will reject the root certificate.</p>
Fingerprint	<p>! IMPORTANT:</p> <p>The fingerprint of the CA root certificate is required when the certificate request mode is Auto, and can be omitted when the certificate request mode is Manual. When it is omitted, no CA root certificate verification occurs automatically and you need to verify the CA server by yourself.</p>
Polling Count	Set the polling interval and attempt limit for querying the certificate request status.
Polling Interval	After an entity makes a certificate request, the CA may need a long period of time if it verifies the certificate request in manual mode. 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.
Enable CRL Checking	Select this box to specify that CRL checking is required during certificate verification.
CRL Update Period	<p>Type the CRL update period, that is, the interval at which the PKI entity downloads the latest CRLs.</p> <p>This item is available when the Enable CRL Checking check box is selected.</p> <p>By default, the CRL update period depends on the next update field in the CRL file.</p>
CRL URL	<p>Type the URL of the CRL distribution point.</p> <p>This item is available when the Enable CRL Checking check box is selected.</p> <p>Note that when the URL of the CRL distribution point is not set, you should acquire the CA certificate and a local certificate, and then acquire a CRL through SCEP.</p> <p>! IMPORTANT:</p> <p>This item does not support domain name resolution.</p>

Return to [Configuration task list for requesting a certificate manually](#).

Return to [Configuration task list for requesting a certificate automatically](#).

Generating an RSA key pair

Select **Authentication** → **PKI** from the navigation tree, and then select the **Certificate** tab to enter the page displaying existing PKI certificates, as shown in [a](#). Then, click **Create Key** to enter RSA key pair parameter configuration page, as shown in [b](#).

a. Certificate configuration page

Entity	Domain	Certificate	CRL	
Domain Name	Issuer	Subject	Certificate Type	Operation
abcd	CN=CA server	CN=CA server	CA	[Delete the certificate][View the certificate]
abcd	CN=CA server	emailAddress=fs,CN=syy,OU=fs,O=fsd,L=fsd,ST=fd,C=CN	Local	[Delete the certificate][View the certificate]

[Create Key](#) [Destroy Key](#) [Retrieve Cert](#) [Request Cert](#)

- There are two ways for requesting and retrieving a certificate manually: online and offline.
- To request a certificate online, you must get the root certificate from the CA server first.
- When you request a certificate offline, the requested information will be displayed on the page first. Please copy it to the CA server to produce the certificate file offline, and then retrieve the file.
- When you delete the CA certificate, the relevant local certificate will also be deleted.

b. Key pair parameter configuration page

Entity	Domain	Certificate	CRL	
--------	--------	-------------	-----	--

Add Key

Key Length: * (512-2048, Default = 1024)

If there is already a key, overwrite it.

Items marked with an asterisk(*) are required

[Apply](#) [Cancel](#)

2. Configuration item for generating an RSA key pair

Item	Description
Key Length	Type the length of the RSA keys.

Return to [Configuration task list for requesting a certificate manually](#).

Destroying the RSA key pair

Select **Authentication** → **PKI** from the navigation tree, and then select the **Certificate** tab to enter the page displaying existing PKI certificates, as shown in [a](#). Click **Destroy Key** to enter RSA key pair destruction page,

as shown in [a](#). Then, click **Apply** to destroy the existing RSA key pair and the corresponding local certificate.

a. Key pair destruction page

Entity	Domain	Certificate	CRL	
--------	--------	-------------	-----	--

Destroy Key

This operation will destroy the key, and corresponding local certificate.

Apply Cancel

Return to [Configuration task list for requesting a certificate manually](#).

Return to [Configuration task list for requesting a certificate automatically](#).

Retrieving a certificate

You can download an existing CA certificate or local certificate from the CA server and save it locally. To do so, you can use two ways: online and offline. In offline mode, you need to retrieve a certificate by an out-of-band means like FTP, disk, e-mail and then import it into the local PKI system.

Select **Authentication** → **PKI** from the navigation tree, and then select the **Certificate** tab to enter the page displaying existing PKI certificates, as shown in [a](#). Click **Retrieve Cert** to enter PKI certificate retrieval page, as shown in [a](#).

a. PKI certificate retrieval page

Entity	Domain	Certificate	CRL	
--------	--------	-------------	-----	--

Retrieve Certificate

Domain Name:

Certificate Type:

Enable Offline Mode

Items marked with an asterisk(*) are required

Apply Cancel

2. Configuration items for retrieving a PKI certificate

Item	Description
Domain Name	Select the PKI domain for the certificate.
Certificate Type	Select the type of the certificate to be retrieved, which can be CA or local.
Enable Offline Mode	Select this check box to retrieve a certificate in offline mode (that is, by an out-of-band means like FTP, disk, or e-mail) and then import the certificate into the local PKI system. The following configuration items are displayed if this check box is selected.
Get File From Device	Specify the path and name of the certificate file.

Item	Description
Get File From PC	<ul style="list-style-type: none"> If the certificate file is saved on the device, select Get File From Device and then specify the path of the file on the device. If the certificate file is saved on a local PC, select Get File From PC and. then specify the path to the file and select the partition of the device for saving the file.
Password	Enter the password for protecting the private key, which was specified when the certificate was exported.

After retrieving a certificate, you can click **View Cert** corresponding to the certificate from the PKI certificates list to display the contents of the certificate, as shown in [a](#).

a. Certificate details

The screenshot shows a window titled "View Certificate Details" with a tabbed interface. The "Certificate" tab is selected. The content displays the following certificate details:

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      064B8D12 262858A7 466C3FE8 A764DBC4
    Signature Algorithm: sha1WithRSAEncryption
    Issuer:
      CN=CA server
    Validity
      Not Before: Jul 25 06:15:18 2008 GMT
      Not After : Jul 25 06:24:43 2013 GMT
    Subject:
      CN=CA server
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
      Modulus (2048 bit):
        00C25190 D3E0039D 0F12D183 12C0229C
        C6A56C93 32723B7C 06C418D4 3824ACE8
        9DEF2B2F E1CB6F7B E77AD16B 4CDC4482
        252F4059 85BC9578 9AE479FC B666371E
        F56D641C 875BA016 5B7B184E CB528721
        99127AFE 7777293F C14ECA11 5436394B
        46B4C4CC 033BF4D8 AC30737A ABDCEB5B
        808C9771 C6EB717C 1C5846DA FDCC0A5C
        8D07B612 F205F79E 4B239793 257630BE
        99AF28BB 55E24B93 23A71866 196EF8E4
        530AB613 17F6A60D 43203708 AE3D50AF
        CA5BBF04 D76FA51A 55A151BD B98A634F
        FCF88AC2 62D81753 13FCF3D7 47BC69F1
        F7BB1868 4E54CBC5 C2DEC1C2 FA047EC6
        6A3A99D8 25768DED F4D0C36F 0C7E555A
        7F75D7CE 3EB14799 62DC2B2A 2651E7B8
        31
      Exponent: 65537 (0x10001)
  
```

Return to [Configuration task list](#) for requesting a certificate manually.

Return to [Configuration task list](#) for requesting a certificate automatically.

Requesting a local certificate

Select **Authentication** → **PKI** from the navigation tree, and then select the **Certificate** tab to enter the page displaying existing PKI certificates, as shown in a. Click **Request Cert** to enter the local certificate request page, as shown in a.

a. Local certificate request page

Entity	Domain	Certificate	CRL	
--------	--------	-------------	-----	--

Request Certificate

Domain Name:

Password: (1-31 Chars.)

Enable Offline Mode

Items marked with an asterisk(*) are required

2. Configuration items for requesting a local certificate

Item	Description
Domain Name	Select the PKI domain for the certificate.
Password	Type the password for certificate revocation.
Enable Offline Mode	Select this check box to request a certificate in offline mode, that is, by an out-of-band means like FTP, disk, or e-mail.

If you select the offline mode and click **Apply**, the offline certificate request information page appears, as shown in a. Submit the information to the CA to request a local certificate.

a. Offline certificate request information page

Entity	Domain	Certificate	CRL	
--------	--------	-------------	-----	--

Offline Certificate Request Information

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBfDCB5gIBADAbMQswCQYDVQQGEwJDTjEMMAoGA1UEAxMDYWFhMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDA/6909wU3SU5fL//aaC4fSM1WdGFav3MreX/1
IAAhYztc1GiTghhMmJhS6aV/t8WV/mL2001Z1rMD+r41bE9/d4Dp8GsVo8E9cHip
Gdu1POQMg1b09c/bafendrKU4i+z9rmfB8VJN2z6dRUtMn5ZFoZb3hWt/S2mP/Z7
ArajIwIDAQABoCIwIAIJKoZIHvcoNAQkOMRMwETAPBgNVHREECDAghwQBAQEKMA0G
CSqGSIb3DQEBAUAA4GBAG4FzUuDu1+fw0Pa+4BYKJV9Ce4W3dmO1jesj5ThofRS
X5chji+sU6r/6d0So1wHH9o28ib7Mgga36IqEprZVxjkpaG9frulBXtf8CFYSSmL
UmbfYiRu94oEvy/xwnzPE9FC1bAfpTubbfxgPsthQL3I9e0LVjI2FFg/bLwCbB20
-----END CERTIFICATE REQUEST-----
```

Return to [Configuration task list for requesting a certificate manually](#).

Retrieving and displaying a CRL

Select **Authentication** → **PKI** from the navigation tree, and then select the **CRL** tab to enter the page displaying CRLs, as shown in [a](#).

a. CRL page

Entity	Domain	Certificate	CRL
Domain Name		Operation	
abcd		[Retrieve CRL][View CRL]	

- Click **Retrieve CRL** to retrieve the CRL of a domain.
- Then, click **View CRL** for the domain to display the contents of the CRL, as shown in [b](#).

b. CRL details

Entity	Domain	Certificate	CRL
--------	--------	-------------	-----

View CRL Details

```
Certificate Revocation List (CRL):
Version 2 (0x1)
Signature Algorithm: sha1WithRSAEncryption
Issuer:
  C=cn
  O=c1
  OU=c1
  CN=c1
Last Update: Oct 25 07:34:16 2007 GMT
Next Update: NONE
CRL extensions:
  X509v3 CRL Number:
  7
  X509v3 Authority Key Identifier:
  keyid:BD5D0565 E744AA19 EA41A2E8 69BE59A5 F62E6C10
```

```
No Revoked Certificates.
Signature Algorithm: sha1WithRSAEncryption
C7E6F3E1 3547818E 84C25849 4E15995C
44A190F4 59885C1D EZ4E16AC A10665A4
027F9CFF 315DB401 14F09629 CEA28DE3
C048235B 93B9CBA6 8F250C94 AEB91AE
10028062 8B2AED6A 5AC4ED1F A1E851A3
C5EBEA4D 76DBF0F1 7BF5D609 0643F930
8356BB7D 2EF341F3 52A5569F 9A85FB10
D2177A49 6DC5C2ED 0F1276E5 4A89E524
```

[Back](#)

2. Description about some fields of the CRL details

Field	Description
Version	CRL version number
Signature Algorithm	Signature algorithm that the CRL uses
Issuer	CA that issued the CRL

Field	Description
X509v3 Authority Key Identifier	Identifier of the CA that issued the certificate and the certificate version (X509v3).
keyid	Public key identifier A CA may have multiple key pairs, and this field identifies which key pair is used for the CRL signature.

Return to [Configuration task list for requesting a certificate manually](#).

Return to [Configuration task list for requesting a certificate automatically](#).

PKI configuration example

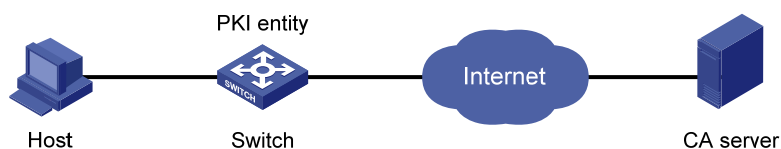
Configuring a PKI entity to request a certificate from a CA

Network requirements

As shown in [a](#), configure the Switch working as the PKI entity, so that:

- The Switch submits a local certificate request to the CA server, which runs the RSA Keon software.
- The Switch acquires CRLs for certificate verification.

a. Network diagram for configuring a PKI entity to request a certificate from a CA



Configuration procedure

Table 145 Configure the CA server

Create a CA server named **myca**.

In this example, you need to configure the basic attributes of **Nickname** and **Subject DN** 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 may use the default values.

Configure extended attributes

After configuring the basic attributes, you need to 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 publishing behavior

After completing the above configuration, you need to perform CRL related configurations.

In this example, select the local CRL publishing mode of HTTP and set the HTTP URL to `http://4.4.4.133:447/myca.crl`.

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

Table 146 Configure Switch

Create a PKI entity.

- Select **Authentication** → **PKI** from the navigation tree. The PKI entity list page is displayed by default. Click **Add** on the page, as shown in **b**, and then perform the following configurations as shown in **c**.

b. PKI entity list

Entity	Domain	Certificate	CRL						
Entity Name	Common Name	FQDN	Country/Region Code	State	Locality	Organization	Organization Unit	IP Address	Operation
<input type="button" value="Add"/>									

c. Configure a PKI entity

Entity	Domain	Certificate	CRL	
Add PKI Entity				
Entity Name:	<input type="text" value="aaa"/>	* (1-15 Chars.)		
Common Name:	<input type="text" value="ac"/>	* (1-31 Chars.)		
IP Address:	<input type="text"/>			
FQDN:	<input type="text"/>	(1-127 Chars.)		
Country/Region Code:	<input type="text"/>	(Country/Region name symbol, two characters compliant to ISO 3166 standard.)		
State:	<input type="text"/>	(1-31 Chars.)		
Locality:	<input type="text"/>	(1-31 Chars.)		
Organization:	<input type="text"/>	(1-31 Chars.)		
Organization Unit:	<input type="text"/>	(1-31 Chars.)		
Items marked with an asterisk(*) are required				
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

- Type **aaa** as the PKI entity name.
- Type **ac** as the common name.
- Click **Apply**.

Create a PKI domain.

- Select the **Domain** tab, and then click **Add**, as shown in **d**, and then perform the following configurations as shown in **e**.

d. PKI domain list

Entity	Domain	Certificate	CRL	
	Domain Name	CA Identifier	Entity Name	Request Mode
				Operation
				<input type="button" value="Add"/>

e. Configure a PKI domain

Entity	Domain	Certificate	CRL	
Add PKI Domain				
Domain Name:	<input type="text" value="torsa"/> * (1-15 Chars.)			
CA Identifier:	<input type="text" value="myca"/> (1-63 Chars.)			
Entity Name:	<input type="text" value="aaa"/>			
Institution:	<input type="text" value="CA"/>			
Requesting URL:	<input type="text" value="http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337"/> (1-127 Chars.)			
LDAP IP:	<input type="text"/>	Port: <input type="text" value="389"/>	Version: <input type="text" value="2"/>	
Request Mode:	<input type="text" value="Manual"/>			
Hash:	<input type="text" value="MD5"/>			
Fingerprint:	<input type="text"/>			(32 Hex)
<input type="button" value="Hide Advanced Config"/>				
Polling Count:	<input type="text" value="50"/> (1-100, Default = 50)			
Polling Interval:	<input type="text" value="20"/> minutes(5-168, Default = 20)			
<input checked="" type="checkbox"/> Enable CRL Checking				
CRL Update Period:	<input type="text"/>			hours(1-720)
CRL URL:	<input type="text" value="http://4.4.4.133:447/myca.crl"/> (1-127 Chars.)			
Items marked with an asterisk(*) are required				
	<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>		

- Type **torsa** as the PKI domain name.
- Type **myca** as the CA identifier.
- Select **aaa** as the local entity.
- Select **CA** as the authority for certificate request.
- Type **http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337** as the URL for certificate request. The URL must be in the format of http://host:port/Issuing Jurisdiction ID, where Issuing Jurisdiction ID is the hexadecimal string generated on the CA.
- Select **Manual** as the certificate request mode.
- Click **Display Advanced Config** to display the advanced configuration items.
- Select the **Enable CRL Checking** check box.

- Type **http://4.4.4.133:447/myca.crl** as the CRL URL.
- Click **Apply**. A dialog box appears, asking “Fingerprint of the root certificate not specified. No root certificate validation will occur. Continue?” Click **OK**.

Generate an RSA key pair.

- Select the **Certificate** tab, and then click **Create Key**, as shown in [f](#), and perform the configuration as shown in [g](#).

f. Certificate list

Entity	Domain	Certificate	CRL	
Domain Name	Issuer	Subject	Certificate Type	Operation
	Create Key	Destroy Key	Retrieve Cert	Request Cert

- There are two ways for requesting and retrieving a certificate manually: online and offline.
- To request a certificate online, you must get the root certificate from the CA server first.
- When you request a certificate offline, the requested information will be displayed on the page first. Please copy it to the CA server to produce the certificate file offline, and then retrieve the file.
- When you delete the CA certificate, the relevant local certificate will also be deleted.

g. Generate an RSA key pair

Entity	Domain	Certificate	CRL	
Add Key				
Key Length:	<input type="text" value="1024"/>	* (512-2048, Default = 1024)		
If there is already a key, overwrite it.				
Items marked with an asterisk(*) are required				
	Apply	Cancel		

- Click **Apply** to generate an RSA key pair.

Retrieve the CA certificate.

- Select the **Certificate** tab, and then click **Retrieve Cert**, as shown in [h](#), and then perform the following configurations as shown in [i](#).

h. Certificate list

Entity	Domain	Certificate	CRL	
Domain Name	Issuer	Subject	Certificate Type	Operation

Create Key Destroy Key Retrieve Cert Request Cert

- There are two ways for requesting and retrieving a certificate manually: online and offline.
- To request a certificate online, you must get the root certificate from the CA server first.
- When you request a certificate offline, the requested information will be displayed on the page first. Please copy it to the CA server to produce the certificate file offline, and then retrieve the file.
- When you delete the CA certificate, the relevant local certificate will also be deleted.

i. Retrieve the CA certificate

Entity	Domain	Certificate	CRL	
Retrieve Certificate				
Domain Name:	torsa			
Certificate Type:	CA			
<input type="checkbox"/> Enable Offline Mode				
Items marked with an asterisk(*) are required				
		Apply	Cancel	

- Select **torsa** as the PKI domain.
- Select **CA** as the certificate type.
- Click **Apply**.

Request a local certificate.

- Select the **Certificate** tab, and then click **Request Cert**, as shown in [j](#), and then perform the following configurations as shown in [k](#).

j. Certificate list

Entity	Domain	Certificate	CRL	
Domain Name	Issuer	Subject	Certificate Type	Operation
torsa	CN=CA server	CN=CA server	CA	[Delete the certificate][View the certificate]

Create Key Destroy Key Retrieve Cert Request Cert

- There are two ways for requesting and retrieving a certificate manually: online and offline.
- To request a certificate online, you must get the root certificate from the CA server first.
- When you request a certificate offline, the requested information will be displayed on the page first. Please copy it to the CA server to produce the certificate file offline, and then retrieval the file.
- When you delete the CA certificate, the relevant local certificate will also be deleted.

k. Request a local certificate

Entity	Domain	Certificate	CRL
--------	--------	-------------	-----

Request Certificate

Domain Name:

Password: (1-31 Chars.)

Enable Offline Mode

Items marked with an asterisk(*) are required

- Select **torsa** as the PKI domain.
- Select **Password** and then type challenge-word as the password.
- Click **Apply**.

Retrieve the CRL.

- After retrieving a local certificate, select the **CRL** tab.
- Click **Retrieve CRL** of the PKI domain of **torsa**, as shown in l.

l. Retrieve the CRL

Entity	Domain	Certificate	CRL
--------	--------	-------------	-----

Domain Name	Operation
torsa	<input type="button" value="Retrieve CRL"/> <input type="button" value="View CRL"/>

Configuration guidelines

When you configure PKI, note the following guidelines:

- Make sure the clocks of entities and the CA are synchronous. Otherwise, the validity period of certificates will be abnormal.
- The Windows 2000 CA server has some restrictions on the data length of a certificate request. If the PKI entity identity information in a certificate request goes beyond a certain limit, the server will not respond to the certificate request.
- The SCEP plug-in is required when you use the Windows Server as the CA. In this case, you need to specify **RA** as the authority for certificate request when configuring the PKI domain.
- The SCEP plug-in is not required when you use the RSA Keon software as the CA. In this case, you need to specify **CA** as the authority for certificate request when configuring the PKI domain.

Port isolation group configuration

Overview

Usually, Layer 2 traffic isolation is achieved by assigning ports to different VLANs. To save VLAN resources, port isolation is introduced to isolate ports within a VLAN, allowing for great flexibility and security.

HP V1910 Switch Series supports only one isolation group that is created automatically by the system as isolation group 1. You can neither remove the isolation group nor create other isolation groups on such devices.

There is no restriction on the number of ports assigned to an isolation group.

Usually, Layer 2 traffic cannot be forwarded between ports from different VLANs. However, Layer 2 data transmission between ports within and outside the isolation group is supported.

Configuring a port isolation group

Select **Security** → **Port Isolate Group** from the navigation tree and in the page that appears, click the **Modify** tab to enter the page shown in [a](#).

a. Configure a port isolation group

The screenshot displays the configuration interface for a port isolation group on an HP V1910-16G switch. The interface includes a 'Summary' tab and a selected 'Modify' tab. The 'Isolate group ID' is set to 'Select group'. The 'Config type' is set to 'Isolate port'. The 'Select port(s)' section shows a grid of 20 port selection buttons, with 'Select All' and 'Select None' buttons below it. An 'Apply' button is located at the bottom right. Below the port selection is a table with columns for 'Isolate port' and 'Uplink-port'.

Isolate port	Uplink-port

2. Port isolation group configuration items

Item	Description
Config type	<p>Specify the role of the port or ports in the isolation group.</p> <ul style="list-style-type: none">Isolate port: Assign the port or ports to the isolation group as an isolated port or ports.Uplink-port: Assign the port to the isolation group as the uplink port. <p>! IMPORTANT:</p> <p>The uplink port is not supported on HP V1910 Switch Series.</p>
Select port(s)	<p>Select the port(s) you want to assign to the isolation group.</p> <p>You can click ports on the chassis front panel for selection; if aggregation interfaces are configured, they will be listed under the chassis panel for selection.</p>

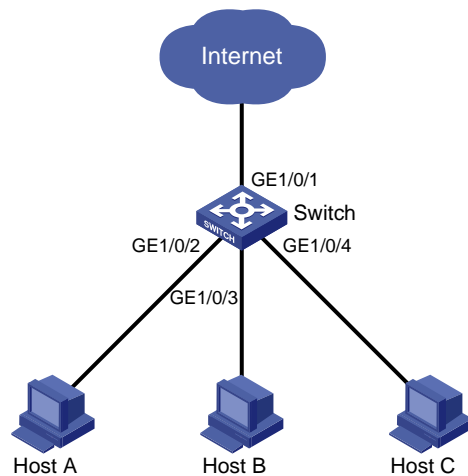
Port isolation group configuration example

Network requirements

- Campus network users Host A, Host B, and Host C are connected to GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 of Switch.
- Switch is connected to the Internet through GigabitEthernet 1/0/1.
- GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 belong to the same VLAN.

Configure Host A, Host B, and Host C to access the Internet and isolate them from each other.

a. Networking diagram for port isolation group configuration



Configuration procedure

Assign GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 to an isolation group as isolated ports.

Select **Security** → **Port Isolate Group** from the navigation tree and in the page that appears, click the **Modify** tab to enter the page shown in a.

a. Configure isolated ports for an isolation group

Summary Modify

Config type Isolate port Uplink-port

Select port(s)

HP V1910-24G-Po...

Aggregation ports

BAGG1

Select All Select None

Apply

Isolate port	Uplink-port
GE1/0/2-GE1/0/4	

- Select **Isolate port** for the port type.
- Select GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4 on the chassis front panel.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration process is complete, click **Close** in the dialog box.

View information about the isolation group.

Click **Summary**. The page shown in **b** appears.

b. Information about port isolation group 1

Summary Modify

Isolate group ID	Uplink-port	Isolate port
1	N/A	GE1/0/2-GE1/0/4

Port type Uplink-port Isolate port

HP V1910-24G-Po...

Aggregation ports

BAGG1

As shown on the page, port isolation group 1 contains these isolated ports: GigabitEthernet 1/0/2, GigabitEthernet 1/0/3, and GigabitEthernet 1/0/4.

Authorized IP configuration

Overview

The authorized IP function is to associate the HTTP or Telnet service with an ACL to filter the requests of clients. Only the clients that pass the ACL filtering can access the device.

Configuring authorized IP

Select **Security** → **Authorized IP** from the navigation tree, and then click the **Setup** tab to enter the authorized IP configuration page, as shown in a.

a. Authorized IP configuration page

Rule ID	Operation	Description	Time Range
---------	-----------	-------------	------------

2. Authorized IP configuration items

Item	Description
Telnet	IPv4 ACL Associate the Telnet service with an IPv4 ACL. You can configure the IPv4 ACL to be selected by selecting QoS → ACL IPv4 .
	IPv6 ACL(Not Supported) Associate the Telnet service with an IPv6 ACL. You can configure the IPv6 ACL to be selected by selecting QoS → ACL IPv6 .
Web (HTTP)	IPv4 ACL Associate the HTTP service with an IPv4 ACL. You can configure the IPv4 ACL to be selected by selecting QoS → ACL IPv4 .

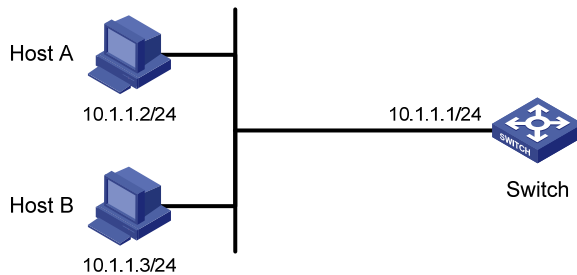
Authorized IP configuration example

Authorized IP configuration example

Network requirements

In [a](#), configure Switch to deny Telnet and HTTP requests from Host A, and permit Telnet and HTTP requests from Host B.

a. Network diagram for authorized IP



Configuration procedure

Create an ACL.

- Select **QoS** → **ACL IPv4** from the navigation tree and then click the **Create** tab to enter the ACL configuration page shown in [a](#).
- Type **2001** for **ACL Number**.
- Click **Apply**.

a. Create an ACL

Summary	Create	Basic Setup	Advanced Setup	Link Setup	Remove
ACL Number	<input type="text" value="2001"/>	2000-2999 for Basic ACL. 3000-3999 for Advanced ACL. 4000-4999 for Ethernet frame header ACL.			
Match Order	<input type="text" value="Config"/>				
<input type="button" value="Apply"/>					

ACL Number	Type	Number of Rules	Match Order

Configure an ACL rule to permit Host B.

- Click the **Basic Setup** tab to enter the page shown in [b](#).

- Select 2001 from the **Select Access Control List (ACL)** drop-down list.
- Select **Permit** from the **Operation** drop-down list.
- Select the **Source IP Address** check box and then type **10.1.1.3**.
- Type **0.0.0.0** in the **Source Wildcard** text box.
- Click **Add**.

b. Configure an ACL rule to permit Host B

Summary	Create	Basic Setup	Advanced Setup	Link Setup	Remove
---------	--------	-------------	----------------	------------	--------

Select Access Control List(ACL)

Configure a Basic ACL

Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation

Check Fragment Check Logging

Source IP Address Source Wildcard

Time Range

Rule ID	Operation	Description	Time Range

Configure authorized IP.

- Select **Security** → **Authorized IP** from the navigation tree and then click the **Setup** tab to enter the authorized IP configuration page shown in **c**.
- Select **2001** for **IPv4 ACL** in the **Telnet** field.
- Select **2001** for **IPv4 ACL** in the **Web(HTTP)** field.
- Click **Apply**.

c. Configure authorized IP

Summary Setup

Telnet

IPv4 ACL : 2001

IPv6 ACL : NoChange

Web(HTTP)

IPv4 ACL : 2001

Apply

Rule ID	Operation	Description	Time Range
---------	-----------	-------------	------------

ACL configuration

ACL overview

With the growth of network scale and network traffic, network security and bandwidth allocation become more and more critical to network management. Packet filtering can be used to efficiently prevent illegal access to networks and to control network traffic and save network resources. One way to implement packet filtering is to use access control lists (ACLs).

An ACL is a set of rules (or a set of permit or deny statements) for determining which packets can pass and which ones should be rejected based on match criteria such as source address, destination address, and port number. ACLs are widely used with technologies such as QoS, where traffic identification is desired.

Introduction to IPv4 ACL

IPv4 ACL classification

IPv4 ACLs, identified by ACL numbers, fall into the following categories, as shown in 1.

1. IPv4 ACL categories

Category	ACL number	Match criteria
Basic IPv4 ACL	2000 to 2999	Source IP address
Advanced IPv4 ACL	3000 to 3999	Source IP address, destination IP address, protocol carried over IP, and other Layer 3 or Layer 4 protocol header information
Ethernet frame header ACL	4000 to 4999	Layer 2 protocol header fields such as source MAC address, destination MAC address, 802.1p precedence, and link layer protocol type

IPv4 ACL match order

An ACL may consist of multiple rules, which specify different match criteria. These match criteria may have overlapping or conflicting parts. The match order determines how packets should be matched against the rules. The comparison of a packet against ACL rules stops immediately after a match is found. The packet is then processed as per the rule.

The following types of IPv4 ACL match orders are available:

- **config**—Compares packets against ACL rules in the order that the rules are configured.
- **auto**—Compares packets against ACL rules in the depth-first match order.

The term depth-first match has different meanings for different types of IPv4 ACLs.

1. Depth-first match for IPv4 ACLs

IPv4 ACL category	Depth-first match procedure
Basic IPv4 ACL	<ol style="list-style-type: none">1. Sort rules by source IP address wildcard mask and compare packets against the rule configured with more zeros in the source IP address wildcard mask.2. In case of a tie, compare packets against the rule configured first.
Advanced IPv4 ACL	<ol style="list-style-type: none">3. Sort rules by the protocol carried over IP. A rule with no limit to the protocol type (that is, configured with the ip keyword) has the lowest precedence. Rules each of which has a single specified protocol type are of the same precedence level.4. If the protocol types have the same precedence, look at the source IP address wildcard mask. Then, compare packets against the rule configured with more zeros in the source IP address wildcard mask.5. If the numbers of zeros in the source IP address wildcard masks are the same, look at their destination IP address wildcard masks. Then, compare packets against the rule configured with more zeros in the destination IP address wildcard mask.6. If the numbers of zeros in the destination IP address wildcard masks are the same, look at the Layer 4 port number ranges, namely the TCP/UDP port number ranges. Then compare packets against the rule configured with the smaller port number range.7. If the port number ranges are the same, compare packets against the rule configured first.
Ethernet frame header ACL	<ol style="list-style-type: none">8. Sort rules by source MAC address mask first and compare packets against the rule configured with more ones in the source MAC address mask.9. If two rules are present with the same number of ones in their source MAC address masks, look at the destination MAC address masks. Then, compare packets against the rule configured with more ones in the destination MAC address mask.10. If the numbers of ones in the destination MAC address masks are the same, compare packets against the one configured first.

Fragments filtering with IPv4 ACLs

Traditional packet filtering performs match operation on only the first fragments. All subsequent non-first fragments are handled in the way the first fragments are handled. This results in security risks, because attackers may exploit this vulnerability to fabricate non-first fragments to attack your network.

As for the configuration of a rule of an IPv4 ACL, you can specify that the rule applies to non-first fragment packets only, and does not apply to non-fragment packets or the first fragment packets. ACL rules that do not contain this keyword are applicable to both non-fragment packets and fragment packets.

Effective period of an ACL

You can control when a rule can take effect by referencing a time range in the rule.

A referenced time range can be one that has not been created yet. The rule, however, can take effect only after the time range is defined and becomes active.

ACL step

NOTE:

The Web interface does not support ACL step configuration.

Meaning of the step

The step defines the difference between two neighboring numbers that are automatically assigned to ACL rules by the device. For example, with a step of 5, rules are automatically numbered 0, 5, 10, 15, and so on. By default, the step is 5.

Whenever the step changes, the rules are renumbered, starting from 0. For example, if four rules are numbered 0, 5, 10, and 15 respectively, changing the step from 5 to 2 will cause the rules to be renumbered 0, 2, 4, and 6.

Benefits of using the step

With the step and rule numbering/renumbering mechanism, you do not need to assign numbers to rules when defining them. The system will assign a newly defined rule a number that is the smallest multiple of the step bigger than the current biggest number. For example, with a step of five, if the biggest number is 28, the newly defined rule will get a number of 30. If the ACL has no rule defined already, the first defined rule will get a number of 0.

Another benefit of using the step is that it allows you to insert new rules between existing ones as needed. For example, after creating four rules numbered 0, 5, 10, and 15 in an ACL with a step of five, you can insert a rule numbered 1.

Configuring an ACL

Configuration task list

Configuring an IPv4 ACL

Perform the tasks in 1 to configure an IPv4 ACL.

1. IPv4 ACL configuration task list

Task	Remarks
Configuring a time range	Optional A rule referencing a time range takes effect only during the specified time range.
Creating an IPv4 ACL	Required The category of the created ACL depends on the ACL number that you specify.
Configuring a rule for a basic IPv4 ACL	Required
Configuring a rule for an advanced IPv4 ACL	Complete one of the three tasks according to the ACL category.
Configuring a rule for an Ethernet frame header ACL	

Configuring a time range

Select **QoS** → **Time Range** from the navigation tree and then select the **Create** tab to enter the time range configuration page, as shown in [a](#).

a. The page for creating a time range

The screenshot shows a configuration page with three tabs: 'Summary', 'Create', and 'Remove'. The 'Create' tab is active. Below the tabs is a text input field for 'Time Range Name' with a '(1-32 Chars.)' label. There are two radio button options: 'Periodic Time Range' and 'Absolute Time Range'. The 'Periodic Time Range' section includes 'Start Time' (0:0) and 'End Time' (24:0) dropdowns, and checkboxes for days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat). The 'Absolute Time Range' section includes 'From' (0:0) and 'To' (24:0) dropdowns, and date dropdowns (1/1/1970 to 12/31/2100). An 'Apply' button is located at the bottom right of the configuration area. Below the configuration area is a 'Summary' section with a large empty box.

[2](#) describes the configuration items for creating a time range.

2. Time range configuration items

Item	Description	
Time Range Name	Set the name for the time range.	
Periodic Time Range	Start Time	Set the start time of the periodic time range.
	End Time	Set the end time of the periodic time range. The end time must be greater than the start time.
	Sun, Mon, Tue, Wed, Thu, Fri, and Sat.	Select the day or days of the week on which the periodic time range is valid. You can select any combination of the days of the week.
Absolute Time Range	From	Set the start time and date of the absolute time range. The time of the day is in the <i>hh:mm</i> format (24-hour clock), and the date is in the <i>MM/DD/YYYY</i> format.

You can define both a periodic time range and an absolute time range to create a compound time range. This compound time range recurs on the day or days

Item	Description
To	Set the end time and date of the absolute time range. The time of the day is in the <i>hh:mm</i> format (24-hour clock), and the date is in the <i>MM/DD/YYYY</i> format. The end time must be greater than the start time.

of the week only within the specified period.

Return to [IPv4 ACL configuration task list](#).

Creating an IPv4 ACL

Select **QoS** → **ACL IPv4** from the navigation tree and then select the **Create** tab to enter the IPv4 ACL configuration page, as shown in [a](#).

a. The page for creating an IPv4 ACL

Summary	Create	Basic Setup	Advanced Setup	Link Setup	Remove
ACL Number	<input type="text"/>	2000-2999 for Basic ACL. 3000-3999 for Advanced ACL. 4000-4999 for Ethernet frame header ACL.			
Match Order	Config <input type="button" value="v"/>				
					<input type="button" value="Apply"/>

ACL Number	Type	Number of Rules	Match Order
2001	Basic	0	Config
3105	Advanced	0	Auto

[2](#) describes the configuration items for creating an IPv4 ACL.

2. IPv4 ACL configuration items

Item	Description
ACL Number	Set the number of the IPv4 ACL.
Match Order	Set the match order of the ACL. Available values are: <ul style="list-style-type: none"> Config—Compare packets against ACL rules in the order that the rules are configured. Auto—Compares packets against ACL rules in the depth-first match order.

Return to [IPv4 ACL configuration task list](#).

Configuring a rule for a basic IPv4 ACL

Select **QoS** → **ACL IPv4** from the navigation tree and then select the **Basic Setup** tab to enter the rule configuration page for a basic IPv4 ACL, as shown in [a](#).

a. The page for configuring an basic IPv4 ACL

Summary	Create	Basic Setup	Advanced Setup	Link Setup	Remove
---------	--------	-------------	----------------	------------	--------

Select Access Control List(ACL)

Configure a Basic ACL

Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation

Check Fragment Check Logging

Source IP Address Source Wildcard

Time Range

Rule ID	Operation	Description	Time Range

2 describes the configuration items for creating a rule for a basic IPv4 ACL.

2. Configuration items for a basic IPv4 ACL rule

Item	Description
Select Access Control List (ACL)	Select the basic IPv4 ACL for which you want to configure rules. Available ACLs are basic IPv4 ACLs that have been configured.
Rule ID	Select the Rule ID option and type a number for the rule. If you do not specify the rule number, the system will assign one automatically.
Operation	Select the operation to be performed for IPv4 packets matching the rule. <ul style="list-style-type: none"> • Permit—Allows matched packets to pass. • Deny—Drops matched packets.
Check Fragment	Select this option to apply the rule to only non-first fragments. If you do not select this option, the rule applies to all fragments and non-fragments.
Check Logging	Select this option to keep a log of matched IPv4 packets. A log entry contains the ACL rule number, operation for the matched packets, protocol that IP carries, source/destination address, source/destination port number, and number of matched packets.
Source IP Address	Select the Source IP Address option and type a source IPv4 address

Item	Description
Source Wildcard	and a wildcard mask, in dotted decimal notation.
Time Range	Select the time range during which the rule takes effect. Available time ranges are those that have been configured.

Return to [IPv4 ACL configuration task list](#).

Configuring a rule for an advanced IPv4 ACL

Select **QoS** → **ACL IPv4** from the navigation tree and then select the **Advanced Setup** tab to enter the rule configuration page for an advanced IPv4 ACL, as shown in [a](#).

a. The page for configuring an advanced IPv4 ACL

Summary	Create	Basic Setup	Advanced Setup	Link Setup	Remove	
---------	--------	-------------	----------------	------------	--------	--

Select Access Control List(ACL) Select an ACL ▼ Help

Configure an Advanced ACL

Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation Permit ▼

Check Fragment Check Logging

IP Address Filter

<input type="checkbox"/> Source IP Address		Source Wildcard	
<input type="checkbox"/> Destination IP Address		Destination Wildcard	

Protocol IP ▼

ICMP Type

Named ICMP Type --- ▼

ICMP Type (0-255) ICMP Code (0-255)

TCP/UDP Port

Check Established

Source: Operator Not Check ▼ Port To Port

Destination: Operator Not Check ▼ Port To Port

(Range of Port is 0-65535)

Precedence Filter

DSCP Not Check ▼

TOS Not Check ▼ Precedence Not Check ▼


Time Range Not Check ▼ Add

Rule ID	Operation	Description	Time Range

2 describes the configuration items for creating a rule for an advanced IPv4 ACL.

2. Configuration items for an advanced IPv4 ACL rule

Item	Description	
Select Access Control List (ACL)	Select the advanced IPv4 ACL for which you want to configure rules. Available ACLs are advanced IPv4 ACLs that have been configured.	
Rule ID	Select the Rule ID option and type a number for the rule. If you do not specify the rule number, the system will assign one automatically.	
Operation	Select the operation to be performed for packets matching the rule. <ul style="list-style-type: none"> • Permit—Allows matched packets to pass. • Deny—Drops matched packets. 	
Check Fragment	Select this option to apply the rule to only non-first fragments. If you do not select this option, the rule applies to all fragments and non-fragments.	
Check Logging	Select this option to keep a log of matched packets. A log entry contains the ACL rule number, operation for the matched packets, protocol that IP carries, source/destination address, source/destination port number, and number of matched packets.	
IP Address Filter	Source IP Address	Select the Source IP Address option and type a source IPv4 address and a source wildcard mask, in dotted decimal notation.
	Source Wildcard	
	Destination IP Address	Select the Source IP Address option and type a source IP address and a source wildcard mask, in dotted decimal notation.
	Destination Wildcard	
Protocol	Select the protocol to be carried by IP. If you select 1 ICMP , you can configure the ICMP message type and code; if you select 6 TCP or 17 UDP , you can configure the TCP or UDP port.	
ICMP Type	Named ICMP Type	Specify the ICMP message type and code. These items are available only when you select 1 ICMP from the Protocol drop-down box.
	ICMP Type	If you select Other from the Named ICMP Type drop-down box, you need to type values in the ICMP Type and ICMP Code fields. Otherwise, the two fields will take the default values, which cannot be changed.
	ICMP Code	
TCP/UDP Port	Check Established	Select this option to make the rule match packets used for establishing and maintaining TCP connections. These items are available only when you select 6 TCP from the Protocol drop-down box.
	Source	Operator Port Select the operators and type the source port numbers and destination port numbers as required.

Item	Description		
	To Port	These items are available only when you select 6 TCP or 17 UDP from the Protocol drop-down box.	
	Operator	Different operators have different configuration requirements for the port number fields: <ul style="list-style-type: none"> • Not Check—The following port number fields cannot be configured. • Range—The following port number fields must be configured to define a port range. • Other values—The first port number field must be configured and the second must not. 	
	Port		
	Destination		
	To Port		
Precedence Filter	DSCP	Specify the DSCP priority.	 IMPORTANT: If you specify the ToS precedence or IP precedence when you specify the DSCP precedence, the specified ToS or IP precedence does not take effect.
	TOS	Specify the ToS precedence.	
	Precedence	Specify the IP precedence.	
Time Range	Select the time range during which the rule takes effect. Available time ranges are those that have been configured.		

Return to [IPv4 ACL configuration task list](#).

Configuring a rule for an Ethernet frame header ACL

Select **QoS** → **ACL IPv4** from the navigation tree and then select the **Link Setup** tab to enter the rule configuration page for an Ethernet frame header IPv4 ACL, as shown in [a](#).

a. The page for configuring a rule for an Ethernet frame header ACL

Summary	Create	Basic Setup	Advanced Setup	Link Setup	Remove	
---------	--------	-------------	----------------	------------	--------	--

Select Access Control List(ACL) Select an ACL ▼ Help

Configure a Link ACL

Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation Permit ▼

MAC Address Filter

Source MAC Address Source Mask

Destination MAC Address Destination Mask

Format of MAC address and Mask is "H-H-H"

COS(802.1p priority) Not Check ▼

Type Filter

LSAP Type (0-FFFF) LSAP Mask (0-FFFF)

Protocol Type (0-FFFF) Protocol Mask (0-FFFF)

Time Range Not Check ▼

Add

Rule ID	Operation	Description	Time Range

2 describes the configuration items for creating a rule for an Ethernet frame header IPv4 ACL.

2. Configuration items for an Ethernet frame header IPv4 ACL rule

Item	Description	
Select Access Control List (ACL)	Select the Ethernet frame header IPv4 ACL for which you want to configure rules. Available ACLs are Ethernet frame header IPv4 ACLs that have been configured.	
Rule ID	Select the Rule ID option and type a number for the rule. If you do not specify the rule number, the system will assign one automatically.	
Operation	Select the operation to be performed for packets matching the rule. <ul style="list-style-type: none"> Permit—Allows matched packets to pass. Deny—Drops matched packets. 	
MAC Address Filter	Source MAC Address ----- Source Mask	Select the Source MAC Address option and type a source MAC address and a mask.
	Destination MAC Address	Select the Destination MAC Address option and type a destination MAC address and a mask.

Item	Description
Destination Mask	
COS(802.1p precedence)	Specify the 802.1p precedence for the rule.
LSAP Type	Select the LSAP Type option and specify the DSAP and SSAP fields in the LLC encapsulation by configuring the following items: <ul style="list-style-type: none"> • LSAP Type—Indicates the frame encapsulation format.
LSAP Mask	<ul style="list-style-type: none"> • LSAP Mask—Indicates the LSAP mask.
Type Filter	
Protocol Type	Select the Protocol Type option and specify the link layer protocol type by configuring the following items: <ul style="list-style-type: none"> • Protocol Type—Indicates the frame type. It corresponds to the type-code field of Ethernet_II and Ethernet_SNAP frames.
Protocol Mask	<ul style="list-style-type: none"> • Protocol Mask—Indicates the protocol mask.
Time Range	Select the time range during which the rule takes effect. Available time ranges are those that have been configured.

Return to [IPv4 ACL configuration task list](#).

Configuration guidelines

When configuring an ACL, follow these guidelines:

Table 147 When defining rules in an ACL, you do not necessarily assign them numbers; the system can do this automatically. For more information, see [ACL step](#).

Table 148 You cannot create a rule with, or modify a rule, to have the same permit/deny statement as an existing rule in the ACL.

Table 149 You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

QoS configuration

Introduction to QoS

Quality of Service (QoS) reflects the ability of a network to meet customer needs. In an Internet, QoS evaluates the ability of the network to forward packets of different services.

The evaluation can be based on different criteria because the network may provide various services. Generally, QoS performance is measured with respect to bandwidth, delay, jitter, and packet loss ratio during packet forwarding process.

Networks without QoS guarantee

On traditional IP networks without QoS guarantee, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. How many resources the packets can obtain completely depends on the time they arrive. This service is called best-effort. It delivers packets to their destinations as possibly as it can, without any guarantee for delay, jitter, packet loss ratio, and so on.

This service policy is only suitable for applications insensitive to bandwidth and delay, such as Word Wide Web (WWW) and E-Mail.

QoS requirements of new applications

The Internet has been growing along with the fast development of networking technologies.

Besides traditional applications such as WWW, E-Mail and FTP, network users are experiencing new services, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together with VPN technologies to carry out operational applications, for instance, to access the database of the company or to monitor remote devices through Telnet.

These new applications have one thing in common, that is, they all have special requirements for bandwidth, delay, and jitter. For example, videoconference and VoD require high bandwidth, low delay and jitter. As for mission-critical applications, such as transactions and Telnet, they may not require high bandwidth but do require low delay and preferential service during congestion.

The emerging applications demand higher service performance of IP networks. Better network services during packets forwarding are required, such as providing dedicated bandwidth, reducing packet loss ratio, managing and avoiding congestion, and regulating network traffic. To meet these requirements, networks must provide more improved services.

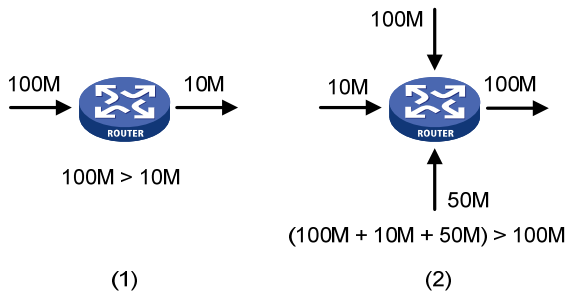
Congestion: causes, impacts, and countermeasures

Network congestion is a major factor contributed to service quality degrading on a traditional network. Congestion is a situation where the forwarding rate decreases due to insufficient resources, resulting in extra delay.

Causes

Congestion easily occurs in complex packet switching circumstances in the Internet. The following figure shows two common cases:

a. Traffic congestion causes



- The traffic enters a device from a high speed link and is forwarded over a low speed link.
- The packet flows enter a device from several incoming interfaces and are forwarded out an outgoing interface, whose rate is smaller than the total rate of these incoming interfaces.

When traffic arrives at the line speed, a bottleneck is created at the outgoing interface causing congestion.

Besides bandwidth bottlenecks, congestion can be caused by resource shortage in various forms such as insufficient processor time, buffer, and memory, and by network resource exhaustion resulting from excessive arriving traffic in certain periods.

Impacts

Congestion may bring these negative results:

- Increased delay and jitter during packet transmission
- Decreased network throughput and resource use efficiency
- Network resource (memory in particular) exhaustion and even system breakdown

It is obvious that congestion hinders resource assignment for traffic and degrades service performance. Congestion is unavoidable in switched networks and multi-user application environments. To improve the service performance of your network, you must address the congestion issues.

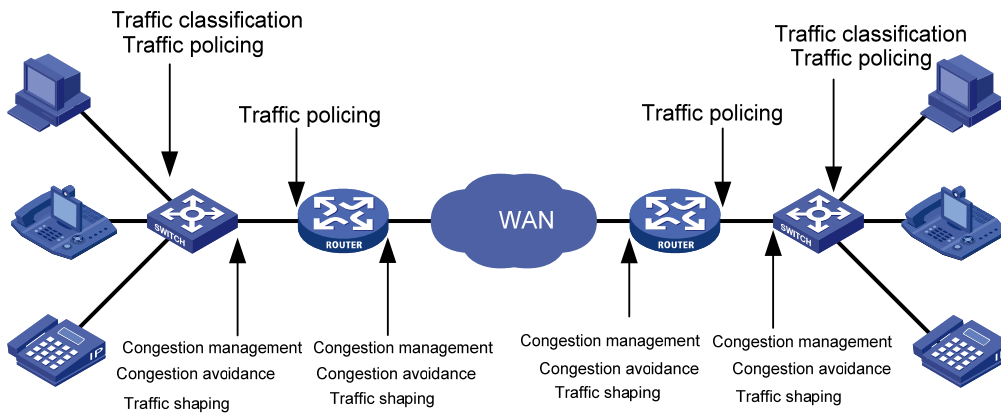
Countermeasures

A simple solution for congestion is to increase network bandwidth, however, it cannot solve all the problems that cause congestion because you cannot increase network bandwidth infinitely.

A more effective solution is to provide differentiated services for different applications through traffic control and resource allocation. In this way, resources can be used more efficiently. During resource allocation and traffic control, the direct or indirect factors that might cause network congestion should be controlled to reduce the probability of congestion. Once congestion occurs, resource allocation should be performed according to the characteristics and demands of applications to minimize the effects of congestion.

End-to-end QoS

a. End-to-end QoS model



As shown in a, traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. Mainly they implement the following functions:

- Traffic classification uses certain match criteria to organize packets with different characteristics into different classes. Traffic classification is usually applied in the inbound direction of a port.
- Traffic policing polices particular flows entering or leaving a device according to configured specifications and can be applied in both inbound and outbound directions of a port. When a flow exceeds the specification, some restrictive measures can be taken to prevent overconsumption of network resources.
- Traffic shaping proactively adjusts the output rate of traffic to adapt traffic to the network resources of the downstream device and avoid unnecessary packet drop and congestion. Traffic shaping is usually applied in the outbound direction of a port.
- Congestion management provides a resource scheduling policy to arrange the forwarding sequence of packets when congestion occurs. Congestion management is usually applied in the outbound direction of a port.
- Congestion avoidance monitors the usage status of network resources and is usually applied in the outbound direction of a port. As congestion becomes worse, it actively reduces the amount of traffic by dropping packets.

Among these QoS technologies, traffic classification is the basis for providing differentiated services. Traffic policing, traffic shaping, congestion management, and congestion avoidance manage network traffic and resources in different ways to realize differentiated services.

Traffic classification

When defining match criteria for classifying traffic, you can use IP precedence bits in the type of service (ToS) field of the IP packet header, or other header information such as IP addresses, MAC addresses, IP protocol field and port numbers. You can define a class for packets with the same quintuple (source address, source port number, protocol number, destination address and destination port number for example), or for all packets to a certain network segment.

When packets are classified on the network boundary, the precedence bits in the ToS field of the IP packet header are generally re-set. In this way, IP precedence can be directly adopted to classify the packets in the network. IP precedence can also be used in queuing to prioritize traffic. The downstream network can either

adopt the classification results from its upstream network or classify the packets again according to its own criteria.

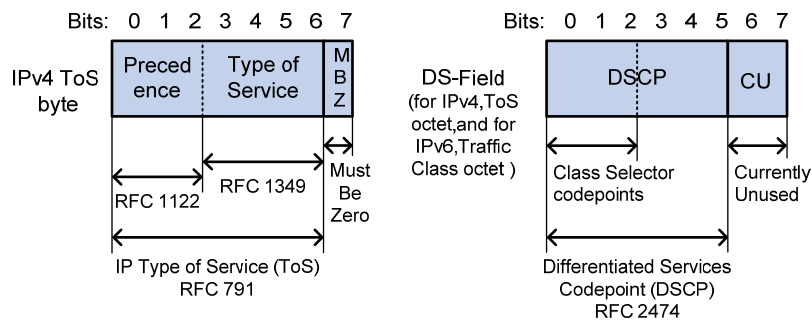
To provide differentiated services, traffic classes must be associated with certain traffic control actions or resource allocation actions. What traffic control actions to adopt depends on the current phase and the resources of the network. For example, CAR is adopted to police packets when they enter the network; GTS is performed on packets when they flow out of the node; queue scheduling is performed when congestion happens; congestion avoidance measures are taken when the congestion deteriorates.

Packet precedences

This section introduces IP precedence, ToS precedence, differentiated services codepoint (DSCP) values, and 802.1p precedence.

Table 150 IP precedence, ToS precedence, and DSCP values

b. DS field and ToS bytes



As shown in [b](#), the ToS field of the IP header contains eight bits: the first three bits (0 to 2) represent IP precedence from 0 to 7; the subsequent four bits (3 to 6) represent a ToS value from 0 to 15. According to RFC 2474, the ToS field of the IP header is redefined as the differentiated services (DS) field, where a DSCP value is represented by the first six bits (0 to 5) and is in the range 0 to 63. The remaining two bits (6 and 7) are reserved.

2. Description on IP Precedence

IP Precedence (decimal)	IP Precedence (binary)	Description
0	000	Routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

In a network in the Diff-Serve model, traffic is grouped into the following four classes, and packets are processed according to their DSCP values.

- Expedited Forwarding (EF) class: In this class, packets are forwarded regardless of link share of other traffic. The class is suitable for preferential services requiring low delay, low packet loss, low jitter, and high bandwidth.

- Assured forwarding (AF) class: This class is divided into four subclasses (AF 1 to AF 4), each containing three drop priorities for more granular classification. The QoS level of the AF class is lower than that of the EF class.
- Class selector (CS) class: This class is derived from the IP ToS field and includes eight subclasses;
- Best effort (BE) class: This class is a special CS class that does not provide any assurance. AF traffic exceeding the limit is degraded to the BE class. All IP network traffic belongs to this class by default.

3. Description on DSCP values

DSCP value (decimal)	DSCP value (binary)	Description
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

Table 151 802.1p precedence

802.1p precedence lies in Layer 2 packet headers and is applicable to occasions where Layer 3 header analysis is not needed and QoS must be assured at Layer 2.

b. An Ethernet frame with an 802.1Q tag header

Destination Address	Source Address	802.1Q header		Length/Type	Data	FCS (CRC-32)
		TPID	TCI			
6 bytes	6 bytes	4 bytes		2 bytes	46 to 1500 bytes	4 bytes

As shown in [b](#), the 4-byte 802.1Q tag header consists of the tag protocol identifier (TPID, two bytes in length), whose value is 0x8100, and the tag control information (TCI, two bytes in length). [c](#) presents the format of the 802.1Q tag header.

c. 802.1Q tag header



The priority in the 802.1Q tag header is called 802.1p precedence, because its use is defined in IEEE 802.1p. [4](#) presents the values for 802.1p precedence.

4. Description on 802.1p precedence

802.1p precedence (decimal)	802.1p precedence (binary)	Description
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

Queue scheduling

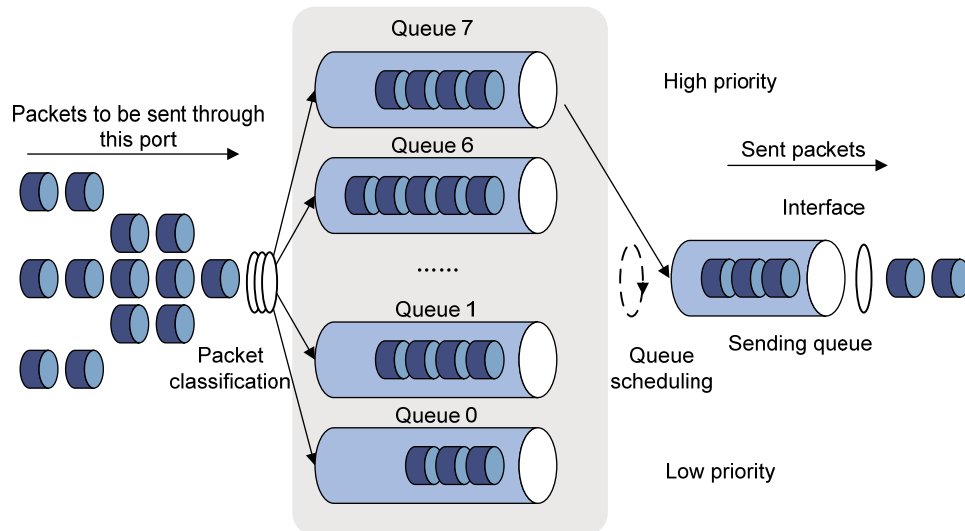
In general, congestion management adopts queuing technology. The system uses a certain queuing algorithm for traffic classification, and then uses a certain precedence algorithm to send the traffic. Each queuing algorithm is used to handle a particular network traffic problem and has significant impacts on bandwidth resource assignment, delay, and jitter.

In this section, two common hardware queue scheduling algorithms Strict Priority (SP) queuing and Weighted Round Robin (WRR) queuing are introduced.

SP queuing

SP queuing is specially designed for mission-critical applications, which require preferential service to reduce response delay when congestion occurs.

a. Schematic diagram for SP queuing



A typical switch provides eight queues per port. As shown in a, SP queuing classifies eight queues on a port into eight classes, numbered 7 to 0 in descending priority order.

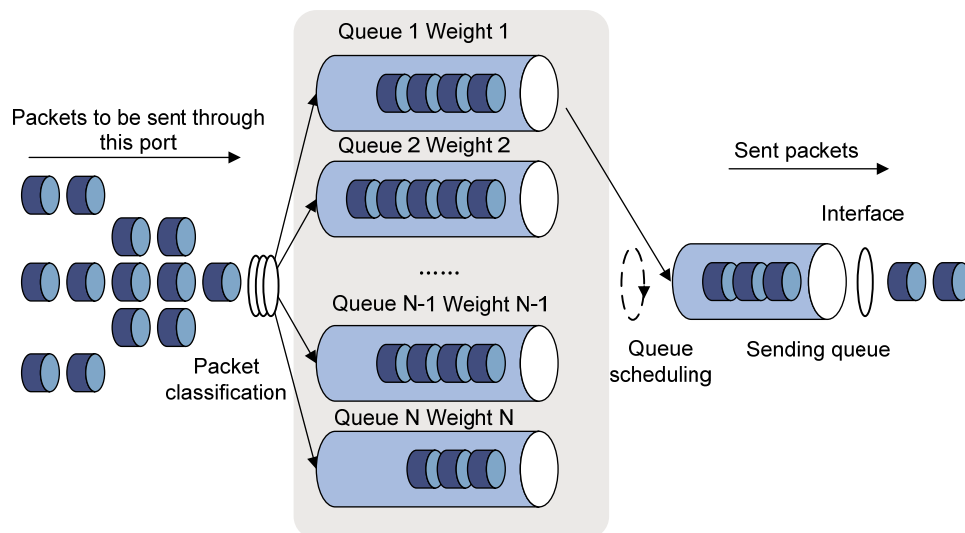
SP queuing schedules the eight queues strictly according to the descending order of priority. It sends packets in the queue with the highest priority first. When the queue with the highest priority is empty, it sends packets in the queue with the second highest priority, and so on. You can assign mission-critical packets to the high priority queue to ensure that they are always served first and common service (such as Email) packets to the low priority queues to be transmitted when the high priority queues are empty.

The disadvantage of SP queuing is that packets in the lower priority queues cannot be transmitted if there are packets in the higher priority queues. This may cause lower priority traffic to never be transmitted.

WRR queuing

WRR queuing schedules all the queues in turn to ensure that every queue can be served for a certain time, as shown in a.

a. Schematic diagram for WRR queuing



A typical switch provides eight output queues per port. WRR assigns each queue a weight value (represented by $w_7, w_6, w_5, w_4, w_3, w_2, w_1, w_0$) to decide the proportion of resources assigned to the

queue. On a 100 Mbps port, you can set the weight values of WRR queuing to 50, 30, 10, 10, 50, 30, 10, and 10 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 respectively). In this way, the queue with the lowest priority is assured of at least 5 Mbps of bandwidth, avoiding the disadvantage of SP queuing that packets in low-priority queues may fail to be served for a long time.

Another advantage of WRR queuing is that while the queues are scheduled in turn, the service time for each queue is not fixed, that is, if a queue is empty, the next queue will be scheduled immediately. This improves bandwidth resource use efficiency.

You can assign the output queues to WRR priority queue group 1 and WRR priority queue group 2. Round robin queue scheduling is performed for group 1 first. If group 1 is empty, round robin queue scheduling is performed for group 2.

NOTE:

You can implement SP+WRR queue scheduling on a port by assigning some queues on the port to the SP scheduling group when configuring WRR. Packets in the SP scheduling group are scheduled preferentially by SP. When the SP scheduling group is empty, the other queues are scheduled by WRR.

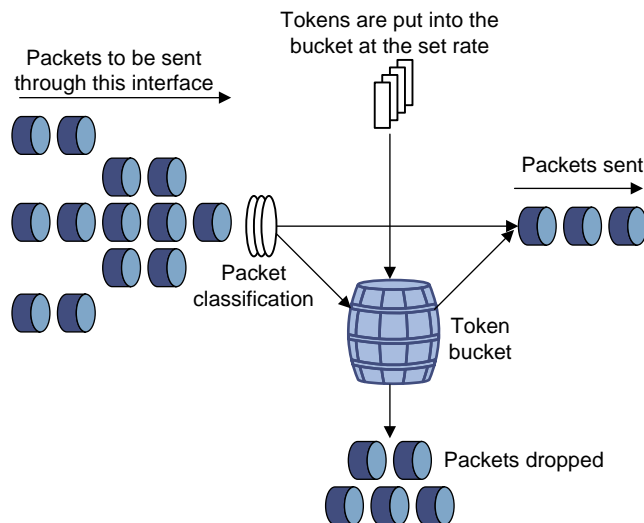
Line rate

Line rate is a traffic control method using token buckets. The line rate of a physical interface specifies the maximum rate for forwarding packets (including critical packets). Line rate can limit all the packets passing a physical interface.

Traffic evaluation and token bucket

A token bucket can be considered as a container holding a certain number of tokens. The system puts tokens into the bucket at a set rate. When the token bucket is full, the extra tokens will cause the token bucket to overflow.

a. Evaluate traffic with the token bucket



The evaluation for the traffic specification is based on whether the number of tokens in the bucket can meet the need of packet forwarding. If the number of tokens in the bucket is enough to forward the packets (generally, one token is associated with a 1-bit forwarding authority), the traffic conforms to the specification, and the traffic is called *conforming traffic*; otherwise, the traffic does not conform to the specification, and the traffic is called *excess traffic*.

A token bucket has the following configurable parameters:

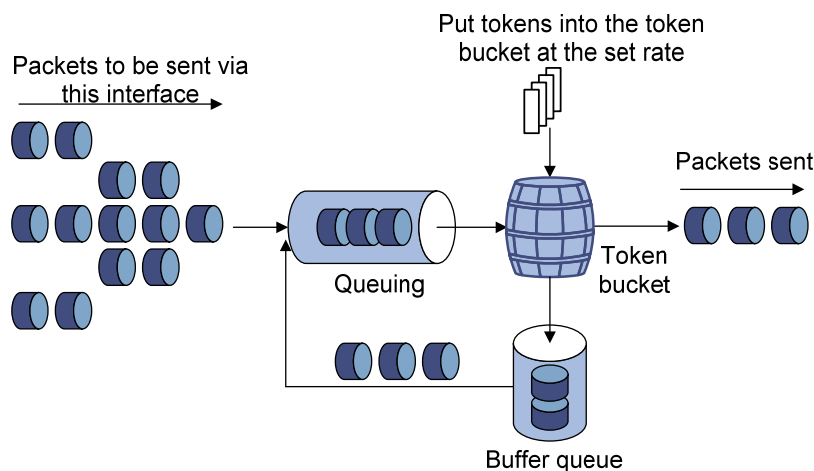
- Mean rate—The rate at which tokens are put into the bucket (the permitted average rate of traffic). It is usually set to the committed information rate (CIR).
- Burst size—The capacity of the token bucket (the maximum traffic size that is permitted in each burst). It is usually set to the committed burst size (CBS). The set burst size must be greater than the maximum packet size.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic conforms to the specification and the corresponding tokens for forwarding the packet are taken away; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excessive.

How line rate works

With line rate configured on an interface, all packets to be sent out the interface are firstly handled by the token bucket of line rate. If enough tokens are available in the token bucket, packets can be forwarded; otherwise, packets are put into QoS queues for congestion management. In this way, the traffic passing the physical interface is controlled.

a. Line rate implementation



With a token bucket used for traffic control, when tokens are available in the token bucket, the bursty packets can be transmitted; if no tokens are available, packets cannot be transmitted until new tokens are generated in the token bucket. In this way, the traffic rate is restricted to the rate for generating tokens, limiting traffic rate and allowing bursty traffic.

Priority mapping

What is priority mapping

When a packet enters a network, it is marked with a certain priority to indicate its scheduling weight or forwarding priority. Then, the intermediate nodes in the network process the packet according to the priority.

When a packet enters a device, the device assigns to the packet a set of predefined parameters (including the 802.1p precedence, DSCP values, IP precedence, and local precedence).

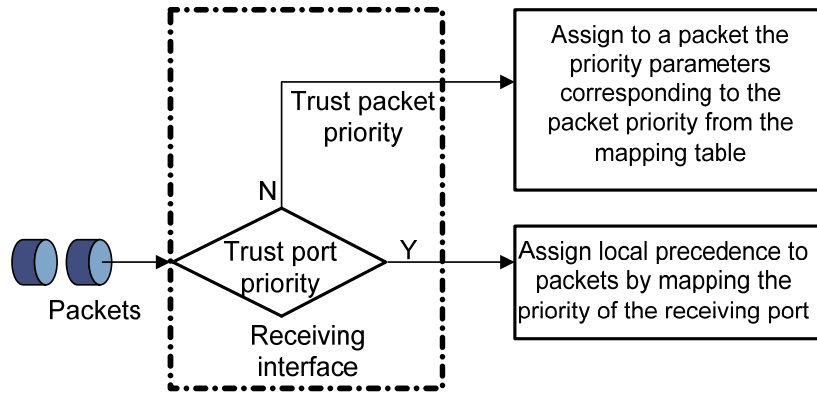
- For more information about 802.1p precedence, DSCP values, and IP precedence, see [Packet precedences](#).
- Local precedence is a locally significant precedence that the device assigns to a packet. A local precedence value corresponds to an output queue. Packets with the highest local precedence are processed preferentially.

The device provides the following priority trust modes on a port:

- Trust packet priority—The device assigns to the packet the priority parameters corresponding to the packet’s priority from the mapping table.
- Trust port priority—The device assigns a priority to a packet by mapping the priority of the receiving port.

You can select one priority trust mode as needed. a shows the process of priority mapping on a device.

a. Priority mapping process



Introduction to priority mapping tables

The device provides various types of priority mapping table, as listed below:

- **CoS to DSCP:** 802.1p-to-DSCP priority mapping table.
- **CoS to Queue:** 802.1p-to-local priority mapping table.
- **DSCP to CoS:** DSCP-to-802.1p priority mapping table, which is applicable to only IP packets.
- **DSCP to DSCP:** DSCP-to-DSCP priority mapping table, which is applicable to only IP packets.
- **DSCP to Queue:** DSCP-to-local priority mapping table, which is applicable to only IP packets.

1 through 2 list the default priority mapping tables.

1. The default CoS to DSCP/CoS to Queue mapping table

Input CoS value	Local precedence (Queue)	DSCP
0	2	0
1	0	8
2	1	16
3	3	24
4	4	32
5	5	40
6	6	48
7	7	56

2. The default DSCP to CoS/DSCP to Queue mapping table

Input DSCP value	Local precedence (Queue)	CoS
0 to 7	0	0
8 to 15	1	1
16 to 23	2	2
24 to 31	3	3
32 to 39	4	4
40 to 47	5	5
48 to 55	6	6
56 to 63	7	7

NOTE:

In the default DSCP to DSCP mapping table, an input value yields a target value equal to it.

QoS configuration

Configuration task lists

Configuring a QoS policy

A QoS policy defines the shaping, policing, or other QoS actions to take on different classes of traffic. It is a set of class-behavior associations.

A class is a set of match criteria for identifying traffic, and it uses the AND or OR operator:

- If the operator is AND, a packet must match all the criteria to match the class.
- If the operator is OR, a packet matches the class if it matches any of the criteria in the class.

A traffic behavior defines a set of QoS actions to take on packets, such as priority marking and redirect.

By associating a traffic behavior with a class in a QoS policy, you apply the specific set of QoS actions to the class of traffic. You can apply a QoS policy to a port to regulate the incoming traffic of the port. A QoS policy can be applied to multiple ports. Only one policy can be applied in inbound direction of a port.

Perform the tasks in 1 to configure a QoS policy:

1. QoS policy configuration task list

Task	Remarks
Configure a class	Required
	Create a class and specify the operator for the match criteria in the class.
Configure match criteria	Required
	Configure match criteria for the class.

Task	Remarks
	Required Create a traffic behavior.
Configure a traffic behavior	Configuring traffic mirroring and traffic redirecting for a traffic behavior Configuring other actions for a traffic behavior Use either approach Configure various actions for the traffic behavior.
	Required Create a policy.
Configure a policy	Configuring classifier-behavior associations for the policy Required Associate the traffic behavior with the class in the QoS policy. A class can be associated with only one traffic behavior in a QoS policy. Associating a class that is already associated with a traffic behavior will overwrite the old association.
Apply the policy	Applying a policy to a port Required Apply the QoS policy to a port.

Configuring queue scheduling

Perform the task in 1 to configure queue scheduling.

1. Queue scheduling configuration task list

Task	Remarks
Configuring queue scheduling on a port	Optional Configure the queue scheduling mode for a port.

Configuring line rate

Perform the task in 1 to configure line rate.

1. Line rate configuration task list

Task	Remarks
Configuring line rate on a port	Required Limit the rate of incoming packets or outgoing packets of a physical port.

Configuring the priority mapping tables

Perform the task in 1 to configure the priority mapping tables:

1. Priority mapping table configuration task list

Task	Remarks
Configuring priority mapping tables	Required Set priority mapping tables.

Configuring priority trust mode

Perform the task in 1 to configure priority trust mode:

1. Priority trust mode configuration task list

Task	Remarks
Configuring priority trust mode on a port	Required Set the priority trust mode of a port.

Creating a class

Select **QoS** → **Classifier** from the navigation tree and click **Create** to enter the page for creating a class, as shown in a.

a. The page for creating a class

Summary	Create	Setup	Remove
Classifier Name	<input type="text"/>	(1-31 Chars.)	
Operator	And	▼	
<input type="button" value="Create"/>			

Classifier Name	Operator	Rule Count
class1	And	0

2 shows the configuration items of creating a class.

2. Configuration items of creating a class

Item	Description
Classifier Name	Specify a name for the classifier to be created.
Operator	Specify the operator for the match criteria of the classifier. <ul style="list-style-type: none">• and—A packet must match all the criteria to match the class.• or—A packet matches the class if it matches any of the criteria in the class.

Return to [QoS policy configuration task list](#).

Configuring match criteria

Select **QoS** → **Classifier** from the navigation tree and click **Setup** to enter the page for setting a class, as shown in a.

a. The page for configuring match criteria

Summary	Create	Setup	Remove
---------	--------	-------	--------

Please select a classifier Select a classifier ▼

Any

DSCP (0-63, you can input 8 entries, for example, 3, 5-7)

IP Precedence (0-7, you can input 8 entries, for example, 3, 5-7)

Classifier (1-31 Chars.)

Inbound Interface

RTP Port from to (2000-65535)

Dot1p

 Service 802.1p
 Customer 802.1p (0-7, you can input 8 entries, for example, 3, 5-7)

MAC

 Source MAC
 Destination MAC (Format of MAC is "H-H-H")

VLAN

 Service VLAN (1-4094, input a range such as 3-20 or up to 8 entries like 3, 5-7)

Customer VLAN (1-4094, input a range such as 3-20 or up to 8 entries like 3, 5-7)

ACL

 ACL IPv4 (2000-4999)

Apply

Rule Type	Rule Value

2 shows the configuration items of configuring match criteria.

2. Configuration items of configuring match criteria

Item	Description
Please select a classifier	Select an existing classifier in the drop-down list.
Any	Define a match criterion to match all packets. Select the option to match all packets.

Item	Description
DSCP	<p>Define a match criterion to match DSCP values.</p> <p>If multiple such match criteria are configured for a class, the new configuration does not overwrite the previous one.</p> <p>You can configure up to eight DSCP values each time. If multiple identical DSCP values are specified, the system considers them as one. The relationship between different DSCP values is OR. After such configurations, all the DSCP values are automatically arranged in ascending order.</p>
IP Precedence	<p>Define a match criterion to match IP precedence values.</p> <p>If multiple such match criteria are configured for a class, the new configuration does not overwrite the previous one.</p> <p>You can configure up to eight IP precedence values each time. If multiple identical IP precedence values are specified, the system considers them as one. The relationship between different IP precedence values is OR. After such configurations, all the IP precedence values are automatically arranged in ascending order.</p>
Customer 802.1p	<p>Define a match criterion to match the customer 802.1p precedence values.</p> <p>If multiple such match criteria are configured for a class, the new configuration does not overwrite the previous one.</p> <p>You can configure up to eight 802.1p precedence values each time. If multiple identical 802.1p precedence values are specified, the system considers them as one. The relationship between different 802.1p precedence values is OR. After such configurations, all the 802.1p precedence values are automatically arranged in ascending order.</p>
MAC	<p>Define a match criterion to match a source MAC address.</p> <p>If multiple such match criteria are configured for a class, the new configuration does not overwrite the previous one.</p> <p>A source MAC address match criterion is significant only to Ethernet interfaces.</p> <hr/> <p>Define a match criterion to match a destination MAC address.</p> <p>If multiple such match criteria are configured for a class, the new configuration does not overwrite the previous one.</p> <p>A destination MAC address match criterion is significant only to Ethernet interfaces.</p>
VLAN	<p>Define a match criterion to match service VLAN IDs.</p> <p>If multiple such match criteria are configured for a class, the new configuration does not overwrite the previous one.</p> <p>You can configure multiple VLAN IDs each time. If the same VLAN ID is specified multiple times, the system considers them as one. The relationship between different VLAN IDs is logical OR. After such a configuration. You can specify VLAN IDs in two ways:</p> <ul style="list-style-type: none"> • Enter a range of VLAN IDs, such as 10-500. The number of VLAN IDs in the range is not limited. • Specify a combination of individual VLAN IDs and VLAN ID ranges, such as 3, 5-7, 10. You can specify up to eight VLAN IDs in this way.

Item	Description
Customer VLAN	<p>Define a match criterion to match customer VLAN IDs.</p> <p>If multiple such match criteria are configured for a class, the new configuration does not overwrite the previous one.</p> <p>You can configure multiple VLAN IDs each time. If the same VLAN ID is specified multiple times, the system considers them as one. The relationship between different VLAN IDs is logical OR. You can specify VLAN IDs in two ways:</p> <ul style="list-style-type: none"> • Enter a range of VLAN IDs, such as 10-500. The number of VLAN IDs in the range is not limited. • Specify a combination of individual VLAN IDs and VLAN ID ranges, such as 3, 5-7, 10. You can specify up to eight VLAN IDs in this way.
ACL IPv4	<p>Define an IPv4 ACL-based match criterion.</p> <p>The ACLs available for selection are existing IPv4 ACLs.</p>

Return to [QoS policy configuration task list](#).

Creating a traffic behavior

Select **QoS** → **Behavior** from the navigation tree and click the **Create** tab to enter the page for creating a traffic behavior, as shown in [a](#).

a. The page for creating a traffic behavior

Summary	Create	Setup	Port Setup	Remove
Behavior Name <input type="text"/> (1-31 Chars.)				
<input type="button" value="Create"/>				
<div style="border: 1px solid #ccc; width: 100%; height: 100%;"></div>				

[2](#) describes the configuration items of creating a behavior.

2. Configuration items of creating a behavior

Item	Description
Behavior name	Specify a name for the behavior to be created.

Return to [QoS policy configuration task list](#).

Configuring traffic mirroring and traffic redirecting for a traffic behavior

Select **QoS** → **Behavior** from the navigation tree and click **Port Setup** to enter the port setup page for a traffic behavior, as shown in a.

a. Port setup page for a traffic behavior

Summary Create Setup **Port Setup** Remove

Please select a behavior

Mirror To Redirect

Please select a port

1 3 5 7 9 11 13 15
2 4 6 8 10 12 14 16 17 18 19 20 HP V1910-16G Sw...

Apply

Behavior Detail

2 describes the traffic mirroring and traffic redirecting configuration items.

2. Traffic mirroring and traffic redirecting configuration items

Item	Description
Please select a behavior	Select an existing behavior in the drop-down list.
Redirect	Set the action of redirecting traffic to the specified destination port.
Please select a port	Specify the port to be configured as the destination port of traffic mirroring or traffic directing on the chassis front panel.

Return to [QoS policy configuration task list](#).

Configuring other actions for a traffic behavior

Select **QoS** → **Behavior** from the navigation tree and click **Setup** to enter the page for setting a traffic behavior, as shown in a.

a. The page for setting a traffic behavior

2 describes the configuration items of configuring other actions for a traffic behavior.

2. Configuration items of configuring other actions for a traffic behavior

Item	Description
Please select a behavior	Select an existing behavior in the drop-down list.
Filter	<p>Configure the packet filtering action.</p> <p>After selecting the Filter option, select one item in the following drop-down list:</p> <ul style="list-style-type: none"> • Permit—Forwards the packet. • Deny—Drops the packet. • Not Set—Cancels the packet filtering action.

Return to [QoS policy configuration task list](#).

Creating a policy

Select **QoS** → **QoS Policy** from the navigation tree and click **Create** to enter the page for creating a policy, as shown in [a](#).

a. The page for creating a policy

Summary Create Setup Remove

Policy Name (1-31 Chars.)

Create

qos

[2](#) describes the configuration items of creating a policy.

2. Configuration items of creating a policy

Item	Description
Policy Name	Specify a name for the policy to be created.

Return to [QoS policy configuration task list](#).

Configuring classifier-behavior associations for the policy

Select **QoS** → **QoS Policy** from the navigation tree and click **Setup** to enter the page for setting a policy, as shown in [a](#).

a. The page for setting a policy

Summary	Create	Setup	Remove
---------	--------	-------	--------

Please select a policy

Classifier Name (1-31 Chars.)

Behavior Name (1-31 Chars.)

Classifier	Behavior
------------	----------

2 describes the configuration items of configuring classifier-behavior associations for the policy.

2. Configuration items of configuring classifier-behavior associations for the policy

Item	Description
Please select a policy	Select a created policy in the drop-down list.
Classifier Name	Select an existing classifier in the drop-down list. The classifiers available for selection are created on the page for creating a classifier.
Behavior Name	Select an existing behavior in the drop-down list. The behaviors available for selection are created on the page for creating a behavior.

Return to [QoS policy configuration task list](#).

Applying a policy to a port

Select **QoS** → **Port Policy** from the navigation tree and click **Setup** to enter the page for applying a policy to a port, as shown in [a](#).

a. The page for applying a policy to a port

2 describes the configuration items of applying a policy to a port.

2. Configuration items of applying a policy to a port

Item	Description
Please select a policy	Select a created policy in the drop-down list.
Direction	Set the direction in which the policy is to be applied. Inbound —Applies the policy to the incoming packets of the specified ports.
Please select port(s)	Click to select ports to which the QoS policy is to be applied on the chassis front panel.

Return to [QoS policy configuration task list](#).

Configuring queue scheduling on a port

Select **QoS** → **Queue** from the navigation tree and click **Setup** to enter the queue scheduling configuration page, as shown in a.

a. The page for configuring queue scheduling

2 describes the configuration items of configuring queue scheduling on a port.

2. Configuration items of configuring queue scheduling on a port

Item	Description
WRR	Enable or disable the WRR queue scheduling mechanism on selected ports. Two options are available: <ul style="list-style-type: none">• Enable—Enables WRR on selected ports.• Not Set—Restores the default queuing algorithm on selected ports.
Queue	Select the queue to be configured. Its value range is 0 to 7, but only 0 to 3 is user configurable and 4 to 7 are reserved.
WRR Setup	Specify the group the current queue is to be assigned to. This drop-down list is available after you select a queue ID. The following groups are available for selection:
Group	<ul style="list-style-type: none">• SP—Assigns a queue to the SP group.• 1—Assigns a queue to WRR group 1.• 2—Assigns a queue to WRR group 2.
Weight	Set a weight for the current queue. This option is available when group 1 or group 2 is selected.
Please select port(s)	Click to select ports to be configured with queuing on the chassis front panel.

Return to [Queue scheduling configuration task list](#).

Configuring line rate on a port

Select **QoS** → **Line rate** from the navigation tree and click the **Setup** tab to enter the line rate configuration page, as shown in [a](#).

a. The page for configuring line rate on a port

Summary
Setup

Please select an interface type GigabitEthernet(L2) ▼

Rate Limit	Enable ▼		Direction	Inbound ▼
CIR	<input type="text"/>	kbps (64-1000000, it must be a multiple of 64)		
<input type="checkbox"/> CBS	<input type="text"/>			
<input type="checkbox"/> EBS	<input type="text"/>			

Please select port(s)

GigabitEthernet1/0/1
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/4
GigabitEthernet1/0/5
GigabitEthernet1/0/6
GigabitEthernet1/0/7
GigabitEthernet1/0/8
GigabitEthernet1/0/9
GigabitEthernet1/0/10

Select All
Select None
Apply

2 describes the configuration items of configuring line rate on a port.

2. Configuration items of configuring line rate on a port

Item	Description
Please select an interface type	Select the types of interfaces to be configured with line rate. The interface types available for selection depend on your device model.
Rate Limit	Enable or disable line rate on the specified port.
Direction	Select a direction in which the line rate is to be applied. <ul style="list-style-type: none"> • Inbound—Limits the rate of packets received on the specified port. • Outbound—Limits the rate of packets sent by the specified port. • Both—Limits the rate of packets received on and sent by the specified port.
CIR	Set the committed information rate (CIR), the average traffic rate.
Please select port(s)	Specify the ports to be configured with line rate Click the ports to be configured with line rate in the port list. You can select one or more ports.

Return to [Line rate configuration task list](#).

Configuring priority mapping tables

Select **QoS** → **Priority Mapping** from the navigation tree to enter the page shown in [a](#).

a. The page for configuring priority mapping tables

Priority Mapping

Mapping Type: CoS to DSCP

Input Value	Output Value	Input Value	Output Value	Input Value	Output Value	Input Value	Output Value
0	0	1	8	2	16	3	24
4	32	5	40	6	48	7	56

Restore Apply Cancel

2 describes the configuration items of configuring priority mapping tables.

2. Configuration items of configuring priority mapping tables

Item	Description
Mapping Type	Select the priority mapping table to be configured, which can be CoS to DSCP, CoS to Queue, DSCP to CoS, DSCP to DSCP, or DSCP to Queue. For example, select DSCP to DSCP mapping type to enter the page shown in 2.
Input Priority Value	Set the output priority value for an input priority value.
Output Priority Value	
Restore	Click Restore to display the default settings of the current priority mapping table on the page. To restore the priority mapping table to the default, click Apply .

a. The page for configuring DSCP to DSCP mapping table

Priority Mapping


Mapping Type: DSCP to DSCP

Input Value	Output Value	Input Value	Output Value	Input Value	Output Value	Input Value	Output Value
0	0	1	1	2	2	3	3
4	4	5	5	6	6	7	7
8	8	9	9	10	10	11	11
12	12	13	13	14	14	15	15
16	16	17	17	18	18	19	19
20	20	21	21	22	22	23	23
24	24	25	25	26	26	27	27
28	28	29	29	30	30	31	31
32	32	33	33	34	34	35	35
36	36	37	37	38	38	39	39
40	40	41	41	42	42	43	43
44	44	45	45	46	46	47	47
48	48	49	49	50	50	51	51
52	52	53	53	54	54	55	55
56	56	57	57	58	58	59	59
60	60	61	61	62	62	63	63

Restore Apply Cancel

Return to [Priority mapping table configuration task list](#).

Configuring priority trust mode on a port

Select **QoS** → **Port Priority** from the navigation tree to enter the page shown in a. Click the  icon corresponding to a port to enter the page shown in b.

a. The page for configuring port priority

Port Priority

Search Item: Keywords:

Interface Name	Priority	Trust Mode	Operation
GigabitEthernet1/0/1	0	Untrust	
GigabitEthernet1/0/2	0	Untrust	
GigabitEthernet1/0/3	0	Untrust	
GigabitEthernet1/0/4	0	Untrust	
GigabitEthernet1/0/5	0	Untrust	
GigabitEthernet1/0/6	0	Untrust	
GigabitEthernet1/0/7	0	Untrust	
GigabitEthernet1/0/8	0	Untrust	
GigabitEthernet1/0/9	0	Untrust	
GigabitEthernet1/0/10	0	Untrust	
GigabitEthernet1/0/11	0	Untrust	
GigabitEthernet1/0/12	0	Untrust	
GigabitEthernet1/0/13	0	Untrust	
GigabitEthernet1/0/14	0	Untrust	
GigabitEthernet1/0/15	0	Untrust	

20 records, 15 per page | page 1/2, record 1-15 |

b. The page for modifying port priority

Port Priority

Interface Name:

Priority:

Trust Mode:

2 describes the port priority configuration items.

2. Port priority configuration items

Item	Description
Interface	The interface to be configured.
Priority	Set a local precedence value for the port.
Trust Mode	Select a priority trust mode for the port: <ul style="list-style-type: none"> Untrust—Not trusts the packet priority. CoS—Trusts the 802.1p precedence of the incoming packets and uses it for priority mapping. DSCP—Trusts the DSCP precedence of the incoming packets and uses it for priority mapping.

[Return to Priority trust mode configuration task list.](#)

Configuration guidelines

When an ACL is referenced to implement QoS, the actions defined in the ACL rules, deny or permit, do not take effect; actions to be taken on packets matching the ACL depend on the traffic behavior definition in QoS.

ACL/QoS configuration examples

ACL/QoS configuration example

Network requirements

As shown in **b**, in the network, the FTP server at IP address 10.1.1.1/24 is connected to the Switch, and the clients access the FTP server through GigabitEthernet 1/0/1 of the Switch.

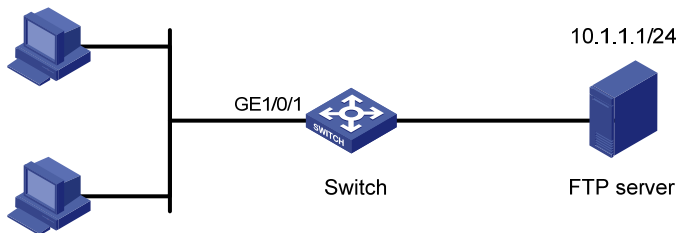
Configure an ACL and a QoS policy as follows to prevent the hosts from accessing the FTP server from 8:00 to 18:00 every day:

Table 152 Create an ACL to prohibit the hosts from accessing the FTP server from 8:00 to 18:00 every day.

Table 153 Configure a QoS policy to drop the packets matching the ACL.

Table 154 Apply the QoS policy in the inbound direction of GigabitEthernet 1/0/1.

b. Network diagram for ACL/QoS configuration



Configuration procedure

Table 155 Configure the time range

Define a time range covering the time range from 8:00 to 18:00 every day.

- Select **QoS** → **Time Range** from the navigation tree and click **Create**.

b. Define a time range covering 8:00 to 18:00 every day

Summary	Create	Remove
---------	---------------	--------

Time Range Name (1-32 Chars.)

Periodic Time Range

Start Time : End Time :

Sun Mon Tue Wed Thu Fri Sat

Absolute Time Range

From : / /

To : / /

Summary

- Type the time range name **test-time**.
- Select the **Periodic Time Range** option, set the **Start Time** to 8:00 and the **End Time** to 18:00, and then select the checkboxes **Sun** through **Sat**.
- Click **Apply**.

Table 156 Define an IPv4 ACL for traffic to the FTP server.

Create an advanced IPv4 ACL.

- Select **QoS** → **ACL IPv4** from the navigation tree and click **Create**.

c. Create an advanced IPv4 ACL

Summary	Create	Basic Setup	Advanced Setup	Link Setup	Remove	
ACL Number	<input type="text" value="3000"/>	2000-2999 for Basic ACL. 3000-3999 for Advanced ACL. 4000-4999 for Ethernet frame header ACL.				
Match Order	<input type="button" value="Config"/> ▼					<input type="button" value="Apply"/>

ACL Number	Type	Number of Rules	Match Order
------------	------	-----------------	-------------

- Type the ACL number 3000.
 - Click **Apply**.
- # Define an ACL rule for traffic to the FTP server.
- Click **Advanced Setup**.

d. Define an ACL rule for traffic to the FTP server

Summary	Create	Basic Setup	Advanced Setup	Link Setup	Remove	
---------	--------	-------------	----------------	------------	--------	--

Select Access Control List(ACL) Help

Configure an Advanced ACL

Rule ID (0-65534, If no ID is entered, the system will specify one.)

Operation

Check Fragment Check Logging

IP Address Filter

Source IP Address Source Wildcard

Destination IP Address Destination Wildcard

Protocol

ICMP Type

Named ICMP Type

ICMP Type (0-255) ICMP Code (0-255)

TCP/UDP Port

Check Established

Source: Operator Port To Port

Destination: Operator Port To Port

(Range of Port is 0-65535)

Precedence Filter

DSCP

TOS Precedence

Time Range Add

Rule ID	Operation	Description	Time Range

- Select ACL 3000 in the drop-down list.
- Select the **Rule ID** option, and type rule ID 2.
- Select **Permit** in the **Operation** drop-down list.
- Select the **Destination IP Address** option, and type IP address 10.1.1.1 and destination wildcard mask 0.0.0.0.
- Select **test-time** in the **Time Range** drop-down list.
- Click **Add**.

Table 157 Configure a QoS policy

Create a class.

- Select **QoS** → **Classifier** from the navigation tree and click **Create**.

e. **Create a class**

Summary	Create	Setup	Remove	
Classifier Name	<input type="text" value="class1"/>	(1-31 Chars.)		
Operator	<input type="text" value="And"/>	▼		
<input type="button" value="Create"/>				

Classifier Name	Operator	Rule Count
-----------------	----------	------------

- Type the class name **class1**.
- Click **Create**.

Define match criteria.

- Click **Setup**.

f. Define match criteria

Summary	Create	Setup	Remove
---------	--------	-------	--------

Please select a classifier

Any

DSCP (0-63, you can input 8 entries, for example, 3, 5-7)

IP Precedence (0-7, you can input 8 entries, for example, 3, 5-7)

Classifier (1-31 Chars.)

Inbound Interface

RTP Port from to (2000-65535)

Dot1p

Service 802.1p Customer 802.1p
(0-7, you can input 8 entries, for example, 3, 5-7)

MAC

Source MAC Destination MAC
(Format of MAC is "H-H-H")

VLAN

Service VLAN (1-4094, input a range such as 3-20 or up to 8 entries like 3, 5-7)

Customer VLAN (1-4094, input a range such as 3-20 or up to 8 entries like 3, 5-7)

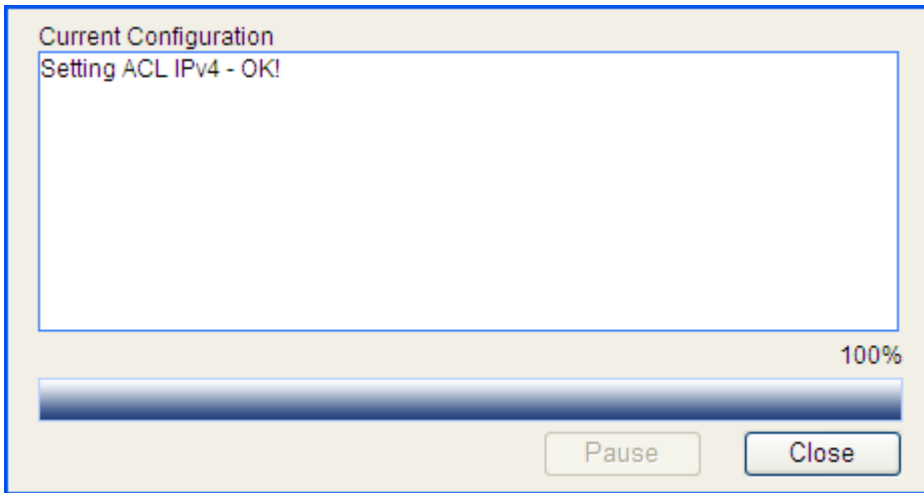
ACL

ACL IPv4 (2000-4999)

Rule Type	Rule Value
-----------	------------

- Select the class name **class1** in the drop-down list.
- Select the **ACL IPv4** option, and select ACL 3000 in the following drop-down list.
- Click **Apply**. A configuration progress dialog box appears, as shown in [g](#).

g. Configuration progress dialog box



- After the configuration is complete, click **Close** on the dialog box.

Create a traffic behavior.

- Select **QoS** → **Behavior** from the navigation tree and click **Create**.

h. Create a traffic behavior

Summary	Create	Setup	Port Setup	Remove
---------	--------	-------	------------	--------

Behavior Name (1-31 Chars.)

- Type the behavior name **behavior1**.
- Click **Create**.

Configure actions for the traffic behavior.

- Click **Setup**.

i. Configure actions for the behavior

Summary	Create	Setup	Port Setup	Remove
---------	--------	-------	------------	--------

Please select a behavior

CAR

Enable Disable

CIR kbps(0-4294967294)

CBS byte(0-4294967294)

Red Discard Pass

Remark

IP Precedence Dot1p

Local Precedence DSCP

Queue

EF Max Bandwidth kbps(8-1000000)

CBS byte(32-2000000)

Percent %(1-100)

CBS-Ratio %(25-500)

AF Max Bandwidth kbps(8-1000000)

Percent %(1-100)

WFQ (16-4096)

Filter Accounting

Behavior Detail

User Defined Behavior Information:
Behavior: behavior1
-none-

- Select **behavior1** in the drop-down list.
 - Select the **Filter** option, and then select **Deny** in the following drop-down list.
 - Click **Apply**. A configuration progress dialog box appears.
 - After the configuration is complete, click **Close** on the dialog box.
- # Create a policy.
- Select **QoS** → **QoS Policy** from the navigation tree and click the **Create** tab.

j. Create a policy

Summary	Create	Setup	Remove
---------	--------	-------	--------

Policy Name (1-31 Chars.)

--

- Type the policy name **policy1**.
 - Click **Create**.
- # Configure classifier-behavior associations for the policy.
- Click **Setup**.

k. Configure classifier-behavior associations for the policy

Summary	Create	Setup	Remove
---------	--------	-------	--------

Please select a policy ▼

Classifier Name ▼ (1-31 Chars.)

Behavior Name ▼ (1-31 Chars.)

Classifier	Behavior

- Select **policy1**.
 - Select **class1** in the **Classifier Name** drop-down list.
 - Select **behavior1** in the **Behavior Name** drop-down list.
 - Click **Apply**.
- # Apply the QoS policy in the inbound direction of GigabitEthernet 1/0/1.
- Select **QoS** → **Port Policy** from the navigation tree and click the **Setup** tab.

I. Apply the QoS policy in the inbound direction of GigabitEthernet 1/0/1

Summary Setup Remove

Please select a policy

Direction

Please select port(s)

1 3 5 7 9 11 13 15
 2 4 6 8 10 12 14 16 17 18 19 20

HP V1910-16G Sw.

Select All Select None

Apply

- Select **policy1** in the **Please select a policy** drop-down list.
- Select **Inbound** in the **Direction** drop-down list.
- Select port GigabitEthernet 1/0/1.
- Click **Apply**. A configuration progress dialog box appears.
- After the configuration is complete, click **Close** on the dialog box.

PoE configuration

NOTE:

Only HP V1910-24G-PoE (365W) Switch JE007A and HP V1910-24G-PoE (170W) Switch JE008A support the PoE function.

PoE overview

Power over Ethernet (PoE) means that power sourcing equipment (PSE) supplies power to powered devices (PDs) from Ethernet interfaces through twisted pair cables.

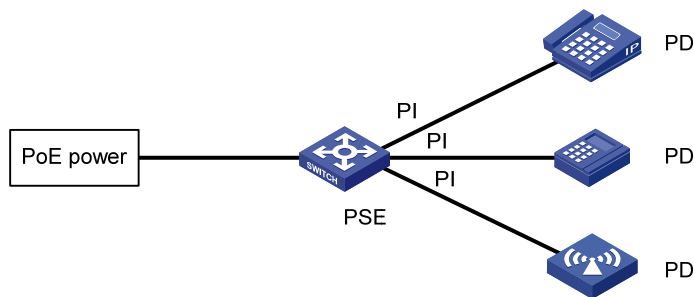
Advantages

- Reliable—Power is supplied in a centralized way so that it is very convenient to provide a backup power supply.
- Easy to connect—A network terminal requires no external power supply but only an Ethernet cable.
- Standard—In compliance with IEEE 802.3af, and a globally uniform power interface is adopted.
- Promising—It can be applied to IP telephones, wireless LAN access points (APs), portable chargers, card readers, web cameras, and data collectors.

Composition

As shown in a, a PoE system consists of PoE power, PSE, power interface (PI), and PD.

a. PoE system diagram



PoE power

The whole PoE system is powered by the PoE power.

PSE

A PSE is a device supplying power for PDs. A PSE can be built-in (Endpoint) or external (Midspan). A built-in PSE is integrated in a switch or router, and an external PSE is independent from a switch or router.

The HP PSEs are built in, and can be classified into two types:

- Device with a single PSE—Only one PSE is available on the device; so the whole device is considered as a PSE.

- Device with multiple PSEs—For a device with multiple PSEs, an interface card with the PoE power supply capability is a PSE. The system uses PSE IDs to identify different PSEs.

NOTE:

HP V1910-24G-PoE (365W) Switch JE007A and HP V1910-24G-PoE (170W) Switch JE008A are devices with a single PSE, so this document describes the device with a single PSE only.

A PSE can examine the Ethernet cables connected to PoE interfaces, search for PDs, classify them, and supply power to them. When detecting that a PD is unplugged, the PSE stops supplying power to the PD.

PI

An Ethernet interface with the PoE capability is called PoE interface. A PoE interface can be an FE or GE interface.

The PSE supplies power for a PoE interface in the following two modes:

- Over signal wires—The PSE uses the pairs (1, 2, 3, 6) for transmitting data in a category 3/5 twisted pair cable to supply DC power while transmitting data to PDs.
- Over spare wires—The PSE uses the pairs (4, 5, 7, 8) not transmitting data in a category 3/5 twisted pair cable to supply DC power to PDs.

NOTE:

HP V1910-24G-PoE (365W) Switch JE007A and HP V1910-24G-PoE (170W) Switch JE008A only support the signal mode.

PD

A PD is a device accepting power from the PSE, including IP phones, wireless APs, chargers of portable devices, POS, and web cameras.

The PD that is being powered by the PSE can be connected to another power supply unit for redundancy power backup.

Protocol specification

The protocol specification related to PoE is IEEE 802.3af.

Configuring PoE

△ CAUTION:

Before configuring PoE, make sure that the PoE power supply and PSE are operating properly; otherwise, you cannot configure PoE or the configured PoE function does not take effect.

Configuring PoE ports

Select **PoE** → **PoE** from the navigation tree and click the **Port Setup** tab, as shown in [a](#).

a. port setup page

Summary
PSE Setup
Port Setup

Select Port:

1

3

5

7

9

11

13

15

17

19

21

23

25

26

27

28

HP V1910-24G-Po...

Select All
Select None

Note: The "Select All" and the "Select None" are only applied to current unit.

Selected

Power Supplied

Power Enabled

Power Disabled

Not Supported

Power Fault

Power State: No Change

Power Max: (1000-30000 milliwatts, step = 100)

Power Priority: No change

Selected Ports:

Apply
Cancel

2. PoE port configuration items

Item	Description
Select Port	Click to select ports to be configured and they will be displayed in the Selected Ports list box.
Power State	<p>Enable or disable PoE on the selected ports.</p> <ul style="list-style-type: none"> The system does not supply power to or reserve power for the PD connected to a PoE port if the PoE port is not enabled with the PoE function. You are allowed to enable PoE for a PoE port if the PoE port will not result in PoE power overload; otherwise, you are not allowed to enable PoE for the PoE port. <p>By default, PoE is disabled on a PoE port.</p> <p>! IMPORTANT:</p> <p>PSE power overload—When the sum of the power consumption of all ports exceeds the maximum power of PSE, the system considers the PSE is overloaded.</p>
Power Max	<p>Set the maximum power for the PoE port.</p> <p>The maximum PoE port power is the maximum power that the PoE port can provide to the connected PD. If the power required by the PD is larger than the maximum PoE port power, the PoE port will not supply power to the PD.</p> <p>By default, the maximum power of a PoE port is 30000 milliwatts.</p>

Item	Description
Power Priority	<p>Set the power supply priority for a PoE port. The priority levels of a PoE port include low, high, and critical in ascending order.</p> <ul style="list-style-type: none"> • When the PoE power is insufficient, power is first supplied to PoE ports with a higher priority level. • When the PSE power is overloaded, the PoE port with a lower priority is first disconnected to guarantee the power supply to the PD with a higher priority. • If you set the priority of a PoE port to critical, the system compares the guaranteed remaining PSE power (the maximum PSE power minus the maximum power allocated to the existing critical PoE port, regardless of whether PoE is enabled for the PoE port) with the maximum power of this PoE port. If the former is greater than the latter, you can succeed in setting the priority to critical, and this PoE port will preempt the power of other PoE ports with a lower priority level; otherwise, you will fail to set the PoE port to critical. In the former case, the PoE ports whose power is preempted will be powered off, but their configurations will remain unchanged. When you change the priority of a PoE port from critical to a lower level, the PDs connecting to other PoE ports will have an opportunity of being powered. <p>By default, the power priority of a PoE port is low.</p> <p>! IMPORTANT:</p> <ul style="list-style-type: none"> • 19 watts guard band is reserved for each PoE port on the device to prevent a PD from being powered off because of a sudden increase of the PD power. When the remaining power of the PSE is lower than 19 watts, the port with a higher priority can preempt the power of the port with a lower priority to ensure the normal working of the higher priority port. • If the sudden increase of the PD power results in PSE power overload, power supply to the PD on the PoE interface with a lower priority is stopped to ensure the power supply to the PD with a higher priority.

Configuring non-standard PD detection

PDs include standard PDs and nonstandard PDs. Standard PDs are those conforming to the IEEE 802.3af standard. Usually, the PSE can detect only standard PDs and supply power to them. The PSE can detect nonstandard PDs and supply power to them only after the PSE is enabled to detect nonstandard PDs.

Select **PoE** → **PoE** from the navigation tree and click the **PSE Setup** tab to enter the page shown in a. The page displays the location of all PSEs, and the status of the non-standard PD detection function.

a. PSE setup

Summary PSE Setup Port Setup		
PSE ID	Location	Non-Standard PD Compatibility
1	subslot 0	Disable ▾

- To enable the non-standard PD detection function of a PSE, find the PSE ID, select **Enable** in the corresponding **Non-Standard PD Compatibility** column, and then click **Apply**.
- To disable the non-standard PD detection function of a PSE, find the PSE ID, select **Disable** in the corresponding **Non-Standard PD Compatibility** column, and then click **Apply**.
- To enable the non-standard PD detection for all PSEs, click **Enable All**.

- To disable the non-standard PD detection for all PSEs, click **Disable All**.

Displaying information about PSE and PoE ports

Select **PoE** → **PoE** from the navigation tree to enter the page of the **Summary** tab. The upper part of the page displays the PSE summary. Click a port on the chassis front panel, and the configuration and power information are displayed in the lower part of the page, as shown in [a](#).


a. PoE summary (with GigabitEthernet 1/0/1 selected)

Summary
PSE Setup
Port Setup

PSE Summary:

PSE ID	Location	State	Max Power (W)	Average Power (W)	Peak Power (W)	Available Power (W)
1	subslot 0	off	370	0	0	370

Ports Power Display:



Port Power State:

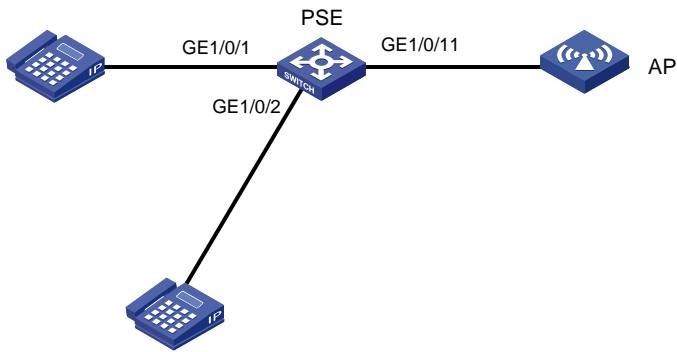
Port	State	Priority	Max Power(mW)	Average Power (mW)	Peak Power (mW)	Free Power (mW)
GE1/0/1	enable	Low	30000	0	0	30000

PoE configuration example

Network requirements

- As shown in [a](#), GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are connected to IP telephones.
- GigabitEthernet 1/0/11 is connected to the AP whose maximum power does not exceed 9000 milliwatts.
- The IP telephones have a higher power supply priority than the AP, so the PSE supplies power to IP telephones first when the PSE power is overloaded.

a. Network diagram for PoE



Configuration procedure

Enable PoE on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, and set their power supply priority to **critical**.

- Select **PoE** → **PoE** from the navigation tree and click the **Setup** tab to perform the following configurations, as shown in a.

a. Configure the PoE ports supplying power to the IP telephones

Summary PSE Setup **Port Setup**

Select Port:

HP V1910-24G-Po...

Select All Select None Note: The "Select All" and the "Select None" are only applied to current unit.

Selected Power Supplied Power Enabled Power Disabled Not Supported Power Fault

Power State: **Enable**

Power Max: (1000-30000 milliwatts, step = 100)

Power Priority: **Critical**

Selected Ports:
GE1/0/1-GE1/0/2

Apply Cancel

- Click to select ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 from the chassis front panel.
- Select **Enable** from the **Power State** drop-down list.
- Select **Critical** from the **Power Priority** drop-down list.
- Click **Apply**.

Enable PoE on GigabitEthernet 1/0/11 and configure the maximum power of the port to 9000 milliwatts.

- Click the **Setup** tab and perform the following configurations, as shown in b.

b. Configure the PoE port supplying power to AP

Summary PSE Setup **Port Setup**

Select Port:

HP V1910-24G-Po...

Select All Select None Note: The "Select All" and the "Select None" are only applied to current unit.

Selected Power Supplied Power Enabled Power Disabled Not Supported Power Fault

Power State:

Power Max: (1000-30000 milliwatts, step = 100)

Power Priority:

Selected Ports:

GE1/0/11

Apply Cancel

- Click to select port GigabitEthernet 1/0/11 from the chassis front panel.
- Select **Enable** from the **Power State** drop-down list.
- Select the check box before **Power Max** and type **9000**.
- Click **Apply**.

After the configuration takes effect, the IP telephones and AP are powered and can work properly.

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

Related information

To find related documents, go to the Manuals page of the HP Business Support Center website:

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

Conventions

This section describes the conventions used in this documentation.

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.

Convention	Description
#	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 Boldface. 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.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/e-updates>

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

Index

A B C D E F G H I L M O P Q R S T V W

A

- AAA configuration example, [358](#)
- ACL overview, [410](#)
- ACL/QoS configuration example, [448](#)
- Architecture of 802.1X, [320](#)
- ARP detection, [315](#)
- ARP overview, [306](#)
- Authorized IP configuration example, [407](#)

B

- Back up configuration, [56](#)
- Basic service setup, [28](#)

C

- CLI commands, [21](#)
- Configuration example for upgrading the system software image at the CLI, [26](#)
- Configuration examples, [334](#)
- Configuration examples, [78](#)
- Configuration guidelines, [203](#)
- Configuration guidelines, [378](#)
- Configuration guidelines, [217](#)
- Configuration guidelines, [421](#)
- Configuration guidelines, [81](#)
- Configuration guidelines, [402](#)
- Configuration guidelines, [447](#)
- Configuration guidelines, [250](#)
- Configuration guidelines, [51](#)
- Configuration guidelines, [15](#)
- Configuration guidelines, [171](#)
- Configuration guidelines, [148](#)
- Configuration guidelines, [86](#)
- Configuration guidelines, [42](#)
- Configuring 802.1X, [329](#)
- Configuring a port, [65](#)
- Configuring a port isolation group, [403](#)
- Configuring a VLAN, [138](#)
- Configuring AAA, [352](#)
- Configuring an ACL, [412](#)
- Configuring and displaying clients' IP-to-MAC bindings, [284](#)
- Configuring authorized IP, [406](#)
- Configuring device basic information, [46](#)
- Configuring DHCP snooping functions on an interface, [293](#)
- Configuring energy saving on a port, [113](#)
- Configuring IGMP snooping, [254](#)

- Configuring IPv4 routing, [267](#)
- Configuring link aggregation and LACP, [208](#)
- Configuring LLDP, [223](#)
- Configuring local port mirroring, [75](#)
- Configuring log management, [52](#)
- Configuring MAC addresses, [173](#)
- Configuring MSTP, [190](#)
- Configuring PKI, [385](#)
- Configuring PoE, [459](#)
- Configuring RADIUS, [368](#)
- Configuring RMON, [97](#)
- Configuring service management, [300](#)
- Configuring stack management, [32](#)
- Configuring storm constrain, [91](#)
- Configuring system time, [48](#)
- Configuring the voice VLAN, [155](#)
- Configuring users, [379](#)
- Configuring VLAN interfaces, [149](#)
- Controlled/uncontrolled port and port authorization status, [320](#)
- Creating a DHCP server group, [282](#)

D

- Device reboot, [60](#)
- DHCP address allocation, [274](#)
- DHCP message format, [276](#)
- DHCP options, [277](#)
- DHCP relay agent configuration example, [285](#)
- DHCP relay agent configuration task list, [280](#)
- DHCP snooping configuration example, [294](#)
- DHCP snooping configuration task list, [290](#)
- DHCP snooping overview, [288](#)
- Diagnostic information, [61](#)
- Diagnostic tool operations, [303](#)
- Displaying clients' IP-to-MAC bindings, [293](#)
- Displaying device summary, [43](#)
- Displaying interface statistics, [133](#)

E

- Electronic label, [61](#)
- Enabling DHCP and configuring advanced parameters for the DHCP relay agent, [281](#)
- Enabling DHCP snooping, [291](#)
- Enabling the DHCP relay agent on an interface, [283](#)

F

- File management configuration, [63](#)

G

Getting started with the CLI, [16](#)
Gratuitous ARP, [313](#)

H

HP implementation of 802.1X, [328](#)

I

IGMP snooping configuration example, [259](#)
Initialize, [58](#)
Initiating 802.1X authentication, [323](#)
Introduction to DHCP, [274](#)
Introduction to DHCP relay agent, [279](#)
Introduction to port mirroring, [74](#)
Introduction to QoS, [422](#)
Introduction to the common items on the web pages, [13](#)
Introduction to the web interface, [4](#)
Introduction to the web-based NM functions, [5](#)

L

Link aggregation and LACP configuration example, [214](#)
LLDP configuration examples, [238](#)
Logging in to the web interface, [2](#)
Logging out of the web interface, [4](#)
Loopback operation, [85](#)

M

MAC address configuration example, [176](#)
Managing ARP entries, [308](#)
Managing users, [82](#)
Monitoring port traffic statistics, [89](#)
MSTP, [185](#)
MSTP configuration example, [199](#)

O

Overview, [251](#)
Overview, [406](#)
Overview, [87](#)
Overview, [28](#)
Overview, [133](#)
Overview, [91](#)
Overview, [85](#)
Overview, [82](#)
Overview, [113](#)
Overview, [403](#)
Overview, [89](#)

Overview, [351](#)

P

PKI configuration example, [397](#)

PKI overview, [383](#)

PoE configuration example, [462](#)

PoE overview, [458](#)

Port isolation group configuration example, [404](#)

Port management configuration example, [70](#)

Precautions, [273](#)

Protocols and standards, [278](#)

Q

QoS configuration, [432](#)

R

RADIUS configuration example, [373](#)

Restore configuration, [56](#)

RMON configuration example, [108](#)

RSTP, [184](#)

S

Save configuration, [57](#)

SNMP configuration, [116](#)

SNMP configuration example, [127](#)

Software upgrade, [59](#)

Stack configuration example, [36](#)

Static route configuration example, [269](#)

STP, [177](#)

System time configuration example, [49](#)

T

Testing cable status, [87](#)

V

VLAN configuration example, [143](#)

Voice VLAN configuration examples, [160](#)

W

Web user level, [5](#)

Web-based network management operating environment, [2](#)