H3C Access Controllers

ACL and QoS Configuration Guide

New H3C Technologies Co., Ltd.
http://www.h3c.com.hk

Document version: 6W102-20190508

Preface

The H3C access controllers documentation set describes the software features for the H3C access controllers and guide you through the software configuration procedures. These guides also provide configuration examples to help you apply software features to different network scenarios.

The *ACL and QoS Configuration Guide* describes ACL, QoS, and time range configurations.

This preface includes the following topics about the documentation:

Hardware and software compatibility matrix

Table 1 Hardware and software compatibility matrix

Hardware series	Model	Product version
WX1800H series	• WX1804H • WX1810H • WX1820H	• WX1804H-CMW710-E5208P03 • WX1810H-CMW710-E5215P01 • WX1820H-CMW710-E5208P03
WX2500H series	• WX2510H • WX2540H • WX2560H	• WX2510H-CMW710-R5215P01 • WX2540H-CMW710-R5215P01 • WX2560H-CMW710-R5215P01
WX3000H series	• WX3010H • WX3010H-L • WX3010H-X • WX3024H • WX3024H-L	• WX3010H-CMW710-R5215P01 • WX3010HL-CMW710-R5215P01 • WX3010HX-CMW710-R5215P01 • WX3024H-CMW710-R5215P01 • WX3024HL-CMW710-R5215P01
WX3500H series	• WX3508H • WX3510H • WX3520H • WX3540H	• WX3508H-CMW710-R5215P01 • WX3510H-CMW710-R5215P01 • WX3520H-CMW710-R5215P01 • WX3540H-CMW710-R5215P01
WX5500E series	• WX5510E • WX5540E	• WX5510E-CMW710-R5215P01 • WX5540E-CMW710-R5215P01
WX5500H series	• WX5540H • WX5560H • WX5580H	• WX5540H-CMW710-R5215P01 • WX5560H-CMW710-R5215P01 • WX5580H-CMW710-R5215P01
Access controller modules	• EWPXM1MAC0F • EWPXM1WCME0 • EWPXM2WCMD0F • LSQM1WCMX20 • LSQM1WCMX40 • LSUM1WCME0	• WCMX40-CMW710-R5215P01 • WCMX40-CMW710-R5215P01 • WCMX20-CMW710-R5215P01 • WCMX20-CMW710-R5215P01 • WCMX40-CMW710-R5215P01 • WCMX40-CMW710-R5215P01

Hardware series	Model	Product version
	• LSUM1WCMX20RT • LSUM1WCMX40RT	• WCMX20-CMW710-R5215P01 • WCMX40-CMW710-R5215P01

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the H3C access controllers.

Conventions

The following information describes the conventions used in the documentation.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; 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

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Wireless terminator unit.
	Wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Documentation feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Contents

Configuring ACLs

Overview

An access control list (ACL) is a set of rules for identifying traffic based on criteria such as source IP address, destination IP address, and port number. The rules are also called permit or deny statements.

ACLs are primarily used for packet filtering. "Configuring packet filtering with ACLs" provides an example. You can use ACLs in QoS, security, routing, and other modules for identifying traffic. The packet drop or forwarding decisions depend on the modules that use ACLs.

ACL types

Type	ACL number	IP version	Match criteria
WLAN client ACL	100 to 199	IPv4 and IPv6	SSID.
WLAN AP ACL	200 to 299	IPv4 and IPv6	AP MAC address and AP serial ID.
Basic ACLs	2000 to 2999	IPv4	Source IPv4 address.
		IPv6	Source IPv6 address.
Advanced ACLs	3000 to 3999	IPv4	Source IPv4 address, destination IPv4 address, packet priority, protocol number, and other Layer 3 and Layer 4 header fields.
		IPv6	Source IPv6 address, destination IPv6 address, packet priority, protocol number, and other Layer 3 and Layer 4 header fields.
Layer 2 ACLs	4000 to 4999	IPv4 and IPv6	Layer 2 header fields, such as source and destination MAC addresses, 802.1p priority, and link layer protocol type.

Numbering and naming ACLs

When creating an ACL, you must assign it a number or name for identification. You can specify an existing ACL by its number or name. Each ACL type has a unique range of ACL numbers.

For an IPv4 basic or advanced ACL, its ACL number or name must be unique in IPv4. For an IPv6 basic or advanced ACL, its ACL number and name must be unique in IPv6. For a Layer 2, WLAN client, or WLAN AP ACL, its number or name must be globally unique.

Match order

The rules in an ACL are sorted in a specific order. When a packet matches a rule, the device stops the match process and performs the action defined in the rule. If an ACL contains overlapping or conflicting rules, the matching result and action to take depend on the rule order.

The following ACL match orders are available:

- **config**—Sorts ACL rules in ascending order of rule ID. A rule with a lower ID is matched before a rule with a higher ID. If you use this method, check the rules and their order carefully.

  NOTE:
  The match order of WLAN client ACLs and WLAN AP ACLs can only be **config**.

- **auto**—Sorts ACL rules in depth-first order. Depth-first ordering makes sure any subset of a rule is always matched before the rule. Table 1 lists the sequence of tie breakers that depth-first ordering uses to sort rules for each type of ACL.

  Table 1 Sort ACL rules in depth-first order

ACL type	Sequence of tie breakers
IPv4 basic ACL	**1.** VPN instance. **2.** More 0s in the source IPv4 address wildcard (more 0s means a narrower IPv4 address range). **3.** Rule configured earlier.
IPv4 advanced ACL	**1.** VPN instance. **2.** Specific protocol number. **3.** More 0s in the source IPv4 address wildcard mask. **4.** More 0s in the destination IPv4 address wildcard. **5.** Narrower TCP/UDP service port number range. **6.** Rule configured earlier.
IPv6 basic ACL	**1.** VPN instance. **2.** Longer prefix for the source IPv6 address (a longer prefix means a narrower IPv6 address range). **3.** Rule configured earlier.
IPv6 advanced ACL	**1.** VPN instance. **2.** Specific protocol number. **3.** Longer prefix for the source IPv6 address. **4.** Longer prefix for the destination IPv6 address. **5.** Narrower TCP/UDP service port number range. **6.** Rule configured earlier.
Layer 2 ACL	**1.** More 1s in the source MAC address mask (more 1s means a smaller MAC address). **2.** More 1s in the destination MAC address mask. **3.** Rule configured earlier.

A wildcard mask, also called an inverse mask, is a 32-bit binary number represented in dotted decimal notation. In contrast to a network mask, the 0 bits in a wildcard mask represent "do care" bits, and the 1 bits represent "don't care" bits. If the "do care" bits in an IP address are identical to the "do care" bits in an IP address criterion, the IP address matches the criterion. All "don't care" bits are

ignored. The 0s and 1s in a wildcard mask can be noncontiguous. For example, 0.255.0.255 is a valid wildcard mask.

Rule numbering

ACL rules can be manually numbered or automatically numbered. This section describes how automatic ACL rule numbering works.

Rule numbering step

If you do not assign an ID to the rule you are creating, the system automatically assigns it a rule ID. The rule numbering step sets the increment by which the system automatically numbers rules. For example, the default ACL rule numbering step is 5. If you do not assign IDs to rules you are creating, they are automatically numbered 0, 5, 10, 15, and so on. The wider the numbering step, the more rules you can insert between two rules.

By introducing a gap between rules rather than contiguously numbering rules, you have the flexibility of inserting rules in an ACL. This feature is important for a config-order ACL, where ACL rules are matched in ascending order of rule ID.

Automatic rule numbering and renumbering

The ID automatically assigned to an ACL rule takes the nearest higher multiple of the numbering step to the current highest rule ID, starting with 0.

For example, if the step is 5, and there are five rules numbered 0, 5, 9, 10, and 12, the newly defined rule is numbered 15. If the ACL does not contain a rule, the first rule is numbered 0.

Whenever the step changes, the rules are renumbered, starting from 0. For example, changing the step from 5 to 2 renumbers rules 5, 10, 13, and 15 as rules 0, 2, 4, and 6.

Fragments filtering with ACLs

Traditional packet filtering matches only first fragments of packets, and allows all subsequent non-first fragments to pass through. Attackers can fabricate non-first fragments to attack networks.

To avoid the risks, the ACL feature is designed as follows:

- Filters all fragments by default, including non-first fragments.
- Allows for matching criteria modification for efficiency. For example, you can configure the ACL to filter only non-first fragments.

Compatibility information

Feature and hardware compatibility

Hardware series	Model	ACL compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	Yes: • WX3010H • WX3010H-X • WX3024H No: • WX3010H-L • WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	Yes
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	Yes

Command and hardware compatibility

The WX1800H series, WX2500H series, and WX3000H series access controllers do not support the **slot** keyword or the *slot-number* argument.

Configuration restrictions and guidelines

Matching packets are forwarded through slow forwarding if an ACL rule contains match criteria or has functions enabled in addition to the following match criteria and functions:

- Source and destination IP addresses.
- Source and destination ports.
- Transport layer protocol.
- ICMP or ICMPv6 message type, message code, and message name.
- VPN instance.
- Logging.
- Time range.

Slow forwarding requires packets to be sent to the control plane for forwarding entry calculation, which affects the device forwarding performance.

Configuration task list

Tasks at a glance

(Required.) Configure ACLs according to the characteristics of the packets to be matched:
• Configuring a basic ACL
  ◦ Configuring an IPv4 basic ACL
  ◦ Configuring an IPv6 basic ACL
• Configuring an advanced ACL
  ◦ Configuring an IPv4 advanced ACL
  ◦ Configuring an IPv6 advanced ACL
• Configuring a Layer 2 ACL
• Configuring a WLAN client ACL
• Configuring a WLAN AP ACL

(Optional.) Copying an ACL
(Optional.) Configuring packet filtering with ACLs

Configuring a basic ACL

This section describes procedures for configuring IPv4 and IPv6 basic ACLs.

Configuring an IPv4 basic ACL

IPv4 basic ACLs match packets based only on source IP addresses.

To configure an IPv4 basic ACL:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IPv4 basic ACL and enter its view.	**acl basic** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]	By default, no ACL exists. The value range for a numbered IPv4 basic ACL is 2000 to 2999. Use the **acl basic** *acl-number* command to enter the view of a numbered IPv4 basic ACL. Use the **acl basic name** *acl-name* command to enter the view of a named IPv4 basic ACL.
3. (Optional.) Configure a description for the IPv4 basic ACL.	**description** *text*	By default, an IPv4 basic ACL does not have a description.
4. (Optional.) Set the rule numbering step.	**step** *step-value*	By default, the rule numbering step is 5 and the start rule ID is 0.
5. Create or edit a rule.	**rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *	By default, an IPv4 basic ACL does not contain any rules.
6. (Optional.) Add or edit a rule comment.	**rule** *rule-id* **comment** *text*	By default, no rule comment is configured.

Configuring an IPv6 basic ACL

IPv6 basic ACLs match packets based only on source IP addresses.

To configure an IPv6 basic ACL:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IPv6 basic ACL view and enter its view.	**acl ipv6 basic** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]	By default, no ACL exists. The value range for a numbered IPv6 basic ACL is 2000 to 2999. Use the **acl ipv6 basic** *acl-number* command to enter the view of a numbered IPv6 basic ACL. Use the **acl ipv6 basic name** *acl-name* command to enter the view of a named IPv6 basic ACL.
3. (Optional.) Configure a description for the IPv6 basic ACL.	**description** *text*	By default, an IPv6 basic ACL does not have a description.
4. (Optional.) Set the rule numbering step.	**step** *step-value*	By default, the rule numbering step is 5 and the start rule ID is 0.

Step	Command	Remarks
5. Create or edit a rule.	**rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **time-range** *time-range-name*] *	By default, an IPv6 basic ACL does not contain any rules.
6. (Optional.) Add or edit a rule comment.	**rule** *rule-id* **comment** *text*	By default, no rule comment is configured.

Configuring an advanced ACL

This section describes procedures for configuring IPv4 and IPv6 advanced ACLs.

Configuring an IPv4 advanced ACL

IPv4 advanced ACLs match packets based on the following criteria:

- Source IP addresses.
- Destination IP addresses.
- Packet priorities.
- Protocol numbers.
- Other protocol header information, such as TCP/UDP source and destination port numbers, TCP flags, ICMP message types, and ICMP message codes.

Compared to IPv4 basic ACLs, IPv4 advanced ACLs allow more flexible and accurate filtering.

To configure an IPv4 advanced ACL:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create an IPv4 advanced ACL and enter its view.	**acl advanced** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]	By default, no ACL exists. The value range for a numbered IPv4 advanced ACL is 3000 to 3999. Use the **acl advanced** *acl-number* command to enter the view of a numbered IPv4 advanced ACL. Use the **acl advanced name** *acl-name* command to enter the view of a named IPv4 advanced ACL.
3. (Optional.) Configure a description for the IPv4 advanced ACL.	**description** *text*	By default, an IPv4 advanced ACL does not have a description.

Step	Command	Remarks
4. (Optional.) Set the rule numbering step.	**step** *step-value*	By default, the rule numbering step is 5 and the start rule ID is 0.
5. Create or edit a rule.	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *	By default, an IPv4 advanced ACL does not contain any rules.
6. (Optional.) Add or edit a rule comment.	**rule** *rule-id* **comment** *text*	By default, no rule comment is configured.

Configuring an IPv6 advanced ACL

IPv6 advanced ACLs match packets based on the following criteria:

- Source IPv6 addresses.
- Destination IPv6 addresses.
- Packet priorities.
- Protocol numbers.
- Other protocol header fields such as the TCP/UDP source port number, TCP/UDP destination port number, ICMPv6 message type, and ICMPv6 message code.

Compared to IPv6 basic ACLs, IPv6 advanced ACLs allow more flexible and accurate filtering.

To configure an IPv6 advanced ACL:

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

Step	Command	Remarks
2. Create an IPv6 advanced ACL and enter its view.	**acl ipv6 advanced** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]	By default, no ACL exists. The value range for a numbered IPv6 advanced ACL is 3000 to 3999. Use the **acl ipv6 advanced** *acl-number* command to enter the view of a numbered IPv6 advanced ACL. Use the **acl ipv6 advanced name** *acl-name* command to enter the view of a named IPv6 advanced ACL.
3. (Optional.) Configure a description for the IPv6 advanced ACL.	**description** *text*	By default, an IPv6 advanced ACL does not have a description.
4. (Optional.) Set the rule numbering step.	**step** *step-value*	By default, the rule numbering step is 5 and the start rule ID is 0.
5. Create or edit a rule.	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* **| any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *	By default, IPv6 advanced ACL does not contain any rules.
6. (Optional.) Add or edit a rule comment.	**rule** *rule-id* **comment** *text*	By default, no rule comment is configured.

Configuring a Layer 2 ACL

Layer 2 ACLs, also called "Ethernet frame header ACLs," match packets based on Layer 2 Ethernet header fields, such as:

- Source MAC address.
- Destination MAC address.
- 802.1p priority (VLAN priority).
- Link layer protocol type.

To configure a Layer 2 ACL:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a Layer 2 ACL and enter its view.	**acl mac** { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]	By default, no ACL exists. The value range for a numbered Layer 2 ACL is 4000 to 4999. Use the **acl mac** *acl-number* command to enter the view of a numbered Layer 2 ACL. Use the **acl mac name** *acl-name* command to enter the view of a named Layer 2 ACL.
3. (Optional.) Configure a description for the Layer 2 ACL.	**description** *text*	By default, a Layer 2 ACL does not have a description.
4. (Optional.) Set the rule numbering step.	**step** *step-value*	By default, the rule numbering step is 5 and the start rule ID is 0.
5. Create or edit a rule.	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *	By default, a Layer 2 ACL does not contain any rules.
6. (Optional.) Add or edit a rule comment.	**rule** *rule-id* **comment** *text*	By default, no rule comment is configured.

Configuring a WLAN client ACL

WLAN client ACLs match packets based on the SSID that the WLAN clients use to access the WLAN. You can use WLAN client ACLs to perform access control on WLAN clients.

To configure a WLAN client ACL:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a WLAN client ACL and enter its view.	**acl wlan client** { *acl-number* | **name** *acl-name* }	By default, no ACL exists. The value range for a numbered WLAN client ACL is 100 to 199. Use the **acl wlan client** *acl-number* command to enter the view of a numbered WLAN client ACL. Use the **acl wlan client name** *acl-name* command to enter the view of a named WLAN client ACL.
3. (Optional.) Configure a description for the WLAN client ACL.	**description** *text*	By default, a WLAN client ACL does not have a description.
4. (Optional.) Set the rule numbering step.	**step** *step-value*	By default, the rule numbering step is 5 and the start rule ID is 0.

Step	Command	Remarks
5. Configure or edit a rule.	**rule** [*rule-id*] { **deny** | **permit** } [**ssid** *ssid-name*]	By default, a WLAN client ACL does not contain any rules.
6. (Optional.) Add or edit a rule comment.	**rule** *rule-id* **comment** *text*	By default, no rule comment is configured.

Configuring a WLAN AP ACL

WLAN AP ACLs match packets from WLAN APs based on the MAC address or serial ID.

To configure a WLAN AP ACL:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a WLAN AP ACL and enter its view.	**acl wlan ap** { *acl-number* | **name** *acl-name* }	By default, no ACL exists. The value range for a numbered WLAN AP ACL is 200 to 299. Use the **acl wlan ap** *acl-number* command to enter the view of a numbered WLAN AP ACL. Use the **acl wlan ap name** *acl-name* command to enter the view of a named WLAN AP ACL.
3. (Optional.) Configure a description for the WLAN AP ACL.	**description** *text*	By default, a WLAN AP ACL does not have a description.
4. (Optional.) Set the rule numbering step.	**step** *step-value*	By default, the rule numbering step is 5 and the start rule ID is 0.
5. Configure or edit a rule.	**rule** [*rule-id*] { **deny** | **permit** } [**mac** *mac-address mac-mask*] [**serial-id** *serial-id*]	By default, a WLAN AP ACL does not contain any rules.
6. (Optional.) Add or edit a rule comment.	**rule** *rule-id* **comment** *text*	By default, no rule comment is configured.

Copying an ACL

You can create an ACL by copying an existing ACL (source ACL). The new ACL (destination ACL) has the same properties and content as the source ACL, but uses a different number or name than the source ACL.

To successfully copy an ACL, make sure:

- The destination ACL number is from the same type as the source ACL number.
- The source ACL already exists, but the destination ACL does not.

To copy an ACL:

Step	Command
1. Enter system view.	**system-view**
2. Copy an existing ACL to create a new ACL.	**acl** [**ipv6** | **mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

Configuring packet filtering with ACLs

This section describes procedures for applying an ACL to filter incoming or outgoing IPv4 or IPv6 packets on the specified interface.

This feature does not take effect on an interface that is an aggregation member port.

Applying an ACL to an interface for packet filtering

The following matrix shows the feature and hardware compatibility:

Hardware series	Model	Feature compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	No
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	Yes
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40	Yes

Hardware series	Model	Feature compatibility
	LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	

To apply an ACL to an interface for packet filtering:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Apply an ACL to the interface to filter packets.	**packet-filter** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }	By default, an interface does not filter packets. You can apply up to 32 ACLs to the same direction of an interface.

Configuring SNMP notifications for packet filtering

You can configure the ACL module to generate SNMP notifications for packet filtering and output them to the information center or SNMP module at the output interval. If an ACL is matched for the first time, the device immediately outputs a notification instead of waiting for the next output. The notification records the number of matching packets and the matched ACL rules.

For more information about the information center and SNMP, see *Network Management and Monitoring Configuration Guide*.

To configure SNMP notifications for packet filtering:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the interval for outputting packet filtering notifications.	**acl trap interval** *interval*	The default setting is 0 minutes. By default, the device does not generate SNMP notifications for packet filtering.

Setting the packet filtering default action

The following matrix shows the feature and hardware compatibility:

Hardware series	Model	Feature compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H	Yes

Hardware series	Model	Feature compatibility
	WX2540H WX2560H	
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	No
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	Yes
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	Yes

To set the packet filtering default action:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the packet filtering default action to deny.	**packet-filter default deny**	By default, the packet filter permits packets that do not match any ACL rule to pass.

Displaying and maintaining ACLs

Execute **display** commands in any view.

Task	Command
Display ACL configuration and match statistics.	**display acl** [**ipv6** | **mac** | **wlan**] { *acl-number* | **all** | **name** *acl-name* }
Display ACL application information for packet filtering.	**display packet-filter interface** [*interface-type interface-number*] [**inbound** | **outbound**] [**slot** *slot-number*]

Task	Command
Display detailed ACL packet filtering information.	**display packet-filter verbose interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]

NOTE:

Support for the **display packet-filter** and **display packet-filter verbose** commands depends on the device model. For more information, see *ACL and QoS Command Reference*.

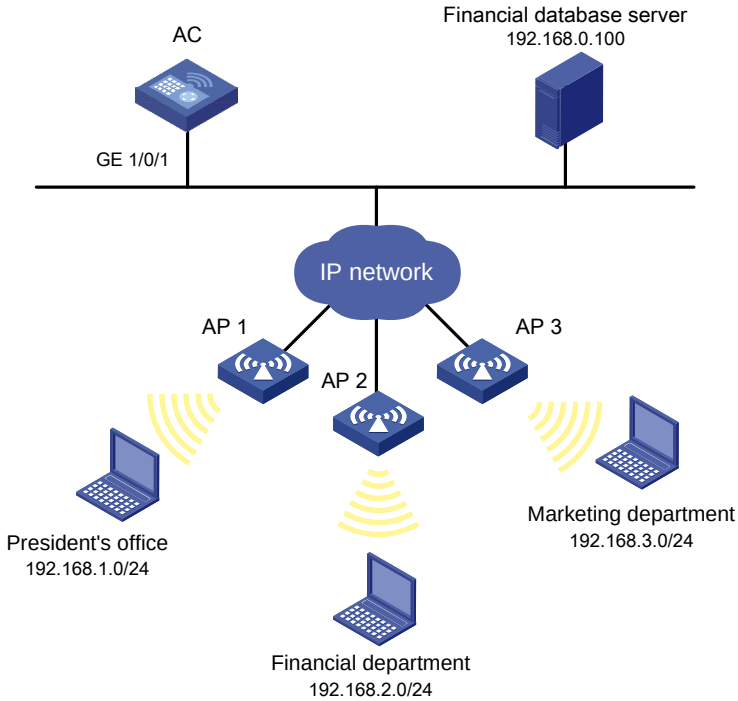
ACL configuration example

Network requirements

A company interconnects its departments through the AC. Configure a packet filter to:

- Permit access from the President's office at any time to the financial database server.
- Permit access from the Financial department to the database server only during working hours (from 8:00 to 18:00) on working days.
- Deny access from any other department to the database server.

Figure 1 Network diagram



Configuration procedure

Create a periodic time range from 8:00 to 18:00 on working days.

```
<AC> system-view
[AC] time-range work 08:0 to 18:00 working-day
```

Create an IPv4 advanced ACL numbered 3000.

```
[AC] acl advanced 3000
```

Configure a rule to permit access from the President's office to the financial database server.

```
[AC-acl-ipv4-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination
192.168.0.100 0
```

Configure a rule to permit access from the Financial department to the database server during working hours.

```
[AC-acl-ipv4-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination
192.168.0.100 0 time-range work
```

Configure a rule to deny access to the financial database server.

```
[AC-acl-ipv4-adv-3000] rule deny ip source any destination 192.168.0.100 0
[AC-acl-ipv4-adv-3000] quit
```

Apply IPv4 advanced ACL 3000 to filter outgoing packets on interface GigabitEthernet 1/0/1.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] packet-filter 3000 outbound
[AC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Verify that a wireless client in the Financial department can ping the database server during working hours. (All clients in this example use Windows XP).

```
C:\> ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time=1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255
Reply from 192.168.0.100: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Verify that a wireless client in the Marketing department cannot ping the database server during working hours.

```
C:\> ping 192.168.0.100
```

```
Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Display configuration and match statistics for IPv4 advanced ACL 3000 on the AC during working hours.

```
[AC] display acl 3000
Advanced IPv4 ACL 3000, 3 rules,
ACL's step is 5
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.100 0
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.0.100 0 time-range work
 rule 10 deny ip destination 192.168.0.100 0
```

The output shows that rule 5 is active.

Contents

QoS overview

In data communications, Quality of Service (QoS) provides differentiated service guarantees for diversified traffic in terms of bandwidth, delay, jitter, and drop rate, all of which can affect QoS.

QoS manages network resources and prioritizes traffic to balance system resources.

The following section describes typical QoS service models and widely used QoS techniques.

Compatibility information

Feature and hardware compatibility

Hardware series	Model	QoS compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	Yes: • WX3010H • WX3010H-X • WX3024H No: • WX3010H-L • WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	Yes
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT	Yes

Hardware series	Model	QoS compatibility
	LSUM1WCMX40RT	

Command and hardware compatibility

The WX1800H series, WX2500H series, WX3000H series access controllers do not support the **slot** keyword or the *slot-number* argument.

QoS service models

This section describes several typical QoS service models.

Best-effort service model

The best-effort model is a single-service model. The best-effort model is not as reliable as other models and does not guarantee delay-free delivery.

The best-effort service model is the default model for the Internet and applies to most network applications. It uses the First In First Out (FIFO) queuing mechanism.

IntServ model

The integrated service (IntServ) model is a multiple-service model that can accommodate diverse QoS requirements. This service model provides the most granularly differentiated QoS by identifying and guaranteeing definite QoS for each data flow.

In the IntServ model, an application must request service from the network before it sends data. IntServ signals the service request with the RSVP. All nodes receiving the request reserve resources as requested and maintain state information for the application flow.

The IntServ model demands high storage and processing capabilities because it requires all nodes along the transmission path to maintain resource state information for each flow. This model is suitable for small-sized or edge networks. However, it is not suitable for large-sized networks, for example, the core layer of the Internet, where billions of flows are present.

DiffServ model

The differentiated service (DiffServ) model is a multiple-service model that can meet diverse QoS requirements. It is easy to implement and extend. DiffServ does not signal the network to reserve resources before sending data, as IntServ does.

QoS techniques overview

The QoS techniques include the following features:

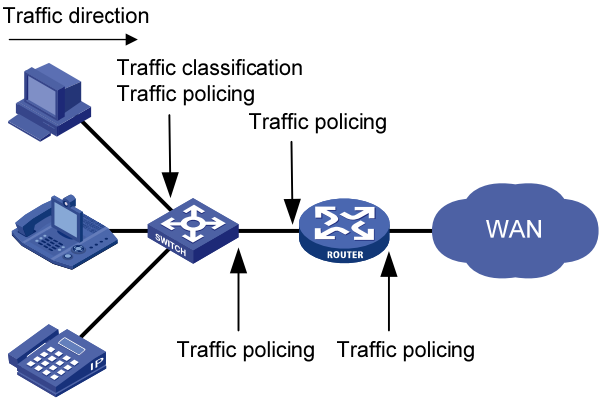
- Traffic classification.
- Traffic policing.

The following section briefly introduces these QoS techniques.

All QoS techniques in this document are based on the DiffServ model.

Deploying QoS in a network

Figure 1 Position of the QoS techniques in a network



As shown in Figure 1, traffic classification and traffic policing mainly implement the following functions:

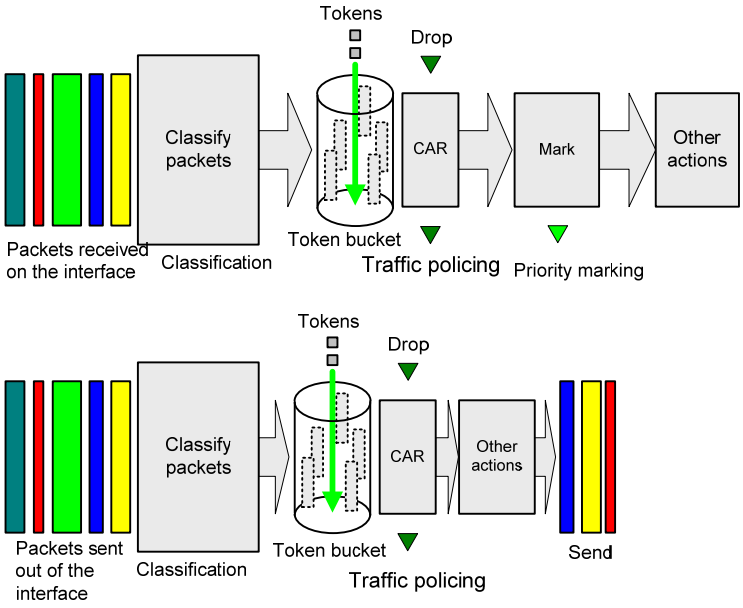
- **Traffic classification**—Uses match criteria to assign packets with the same characteristics to a traffic class. Based on traffic classes, you can provide differentiated services.
- **Traffic policing**—Polices flows and imposes penalties to prevent aggressive use of network resources. You can apply traffic policing to both incoming and outgoing traffic of a port.

QoS processing flow in a device

Figure 2 briefly describes how the QoS module processes traffic.

1. Traffic classifier identifies and classifies traffic for subsequent QoS actions.
2. The QoS module takes various QoS actions on classified traffic as configured, depending on the traffic processing phase and network status. For example, you can configure the QoS module to perform traffic policing for incoming traffic.

Figure 2 QoS processing flow



Configuring a QoS policy

You can configure QoS by using the MQC approach or non-MQC approach. Some features support both approaches, but some support only one.

Non-MQC approach

In the non-MQC approach, you configure QoS service parameters without using a QoS policy.

MQC approach

In the modular QoS configuration (MQC) approach, you configure QoS service parameters by using QoS policies. A QoS policy defines the policing or other QoS actions to take on different classes of traffic. It is a set of class-behavior associations.

A traffic 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 traffic class.
- If the operator is OR, a packet matches the traffic class if it matches any of the criteria in the traffic class.

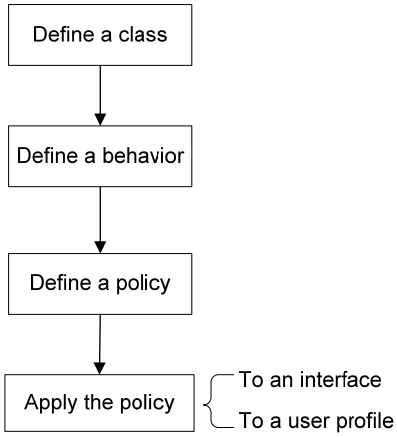
A traffic behavior defines a set of QoS actions to take on packets, such as priority marking.

By associating a traffic behavior with a traffic class in a QoS policy, you apply QoS actions in the traffic behavior to the traffic class.

Configuration procedure diagram

Figure 3 shows how to configure a QoS policy.

Figure 3 QoS policy configuration procedure



Defining a traffic class

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a traffic class and enter traffic class view.	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	By default, no traffic class exists.
3. Configure match criteria.	**if-match** [**not**] *match-criteria*	By default, no match criterion is configured. For more information, see the **if-match** command in *ACL and QoS Command Reference*.

Defining a traffic behavior

A traffic behavior is a set of QoS actions (such as traffic policing and priority marking) to take on a traffic class.

To define a traffic behavior:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*	By default, no traffic behavior exists.
3. Configure actions in the traffic behavior.	See the subsequent chapters, depending on the purpose of the traffic behavior: traffic policing, traffic filtering, and priority marking.	By default, no action is configured for a traffic behavior.

Defining a QoS policy

To perform actions defined in a behavior for a class of packets, associate the behavior with the class in a QoS policy.

To associate a traffic class with a traffic behavior in a QoS policy:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a QoS policy and enter QoS policy view.	**qos policy** *policy-name*	By default, no QoS policy exists.
3. Associate a traffic class with a traffic behavior to create a class-behavior association in the QoS policy.	**classifier** *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]	By default, a traffic class is not associated with a traffic behavior. Repeat this step to create more class-behavior associations.

Applying the QoS policy

You can apply a QoS policy to the following destinations:

- **Interface**—The QoS policy takes effect on the traffic sent or received on the interface.
- **User profile**—The QoS policy takes effect on the traffic sent or received by the online users of the user profile.

You can modify traffic classes, traffic behaviors, and class-behavior associations in a QoS policy even after it is applied. If a traffic class uses an ACL for traffic classification, you can delete or modify the ACL.

Applying the QoS policy to an interface

A QoS policy can be applied to multiple interfaces. However, only one QoS policy can be applied to one direction (inbound or outbound) of an interface.

The QoS policy applied to the outgoing traffic on an interface does not regulate local packets. Local packets refer to critical protocol packets sent by the local system for operation maintenance. The most common local packets include link maintenance, RIP, and SSH packets.

To apply a QoS policy to an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Apply the QoS policy to the interface.	**qos apply policy** *policy-name* { **inbound** | **outbound** }	By default, no QoS policy is applied to an interface.

Applying the QoS policy to a user profile

The following matrix shows the feature and hardware compatibility:

Hardware series	Model	Feature compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes
WX3000H series	WX3010H WX3010H-L WX3010H-X	No

Hardware series	Model	Feature compatibility
	WX3024H WX3024H-L	
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes
WX5500H series	WX5540H WX5560H WX5580H	Yes
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	Yes

You can apply a QoS policy to multiple user profiles. In one direction of each user profile, only one policy can be applied. To modify a QoS policy already applied to a direction, first remove the applied QoS policy.

To apply a QoS policy to a user profile:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter user profile view.	**user-profile** *profile-name*	The configuration made in user profile view takes effect only after it is successfully issued to the driver.
3. Apply the QoS policy.	**qos apply policy** *policy-name* { **inbound** | **outbound** }	Use the **inbound** keyword to apply the QoS policy to the incoming traffic of the device (traffic sent by the online users). Use the **outbound** keyword to apply the QoS policy to the outgoing traffic of the device (traffic received by the online users).

Displaying and maintaining QoS policies

Execute **display** commands in any view.

Task	Command
Display traffic class configuration.	**display traffic classifier** { **system-defined** | **user-defined** } [*classifier-name*] [**slot** *slot-number*]

Task	Command
Display traffic behavior configuration.	**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*] [**slot** *slot-number*]
Display QoS policy configuration.	**display qos policy** { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]
Display information about QoS policies applied to interfaces.	**display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**]
Display information about QoS policies applied to user profiles.	**display qos policy user-profile** [**name** *profile-name*] [**user-id** *user-id*] [**slot** *slot-number*] [**inbound** | **outbound**]

NOTE:

Support for the **display qos policy user-profile** command depends on the device model. For more information, see *ACL and QoS Command Reference*.

Configuring priority mapping

Overview

When a packet arrives, a device assigns a set of QoS priority parameters to the packet based on either of the following:

- A priority field carried in the packet.
- The port priority of the incoming port.

This process is called priority mapping. During this process, the device can modify the priority of the packet according to the priority mapping rules. The set of QoS priority parameters decides the scheduling priority and forwarding priority of the packet.

Priority mapping is implemented with priority maps and involves the following priorities:

- 802.11e priority.
- 802.1p priority.
- DSCP.
- IP precedence.
- Local precedence.

Introduction to priorities

Priorities include the following types: priorities carried in packets, and priorities locally assigned for scheduling only.

Packet-carried priorities include 802.1p priority, DSCP precedence, and IP precedence. These priorities have global significance and affect the forwarding priority of packets across the network. For more information about these priorities, see "Appendixes."

Locally assigned priorities only have local significance. They are assigned by the device only for scheduling. The device supports only local precedence for locally assigned priorities. A local precedence value corresponds to an output queue. A packet with higher local precedence is assigned to a higher priority output queue to be preferentially scheduled.

Priority maps

The device provides various types of priority maps. By looking through a priority map, the device decides which priority value to assign to a packet for subsequent packet processing.

The default priority maps (as shown in Appendix B Default priority maps) are available for priority mapping. They are adequate in most cases. If a default priority map cannot meet your requirements, you can modify the priority map as required.

Priority mapping configuration tasks

You can configure priority mapping by using any of the following methods:

- **Configuring priority trust mode**—In this method, you can configure a port to look up a trusted priority type (802.1p, for example) in incoming packets in the priority maps. Then, the system maps the trusted priority to the target priority types and values.
- **Changing port priority**—If no packet priority is trusted, the port priority of the incoming port is used. By changing the port priority of a port, you change the priority of the incoming packets on the port.

To configure priority mapping, perform the following tasks:

Tasks at a glance
(Optional.) Configuring a priority map
(Required.) Perform one of the following tasks: • Configuring a port to trust packet priority for priority mapping • Changing the port priority of an interface

Configuring a priority map

The device provides the following types of priority map:

Priority map	Description
dot11e-lp	802.11e-local priority map.
dot1p-lp	802.1p-local priority map.
dscp-lp	DSCP-local priority map.
lp-dot11e	Local-802.11e priority map.
lp-dot1p	Local-802.1p priority map.
lp-dscp	Local-DSCP priority map.

To configure a priority map

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter priority map view.	**qos map-table** { **dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp** }	N/A

Step	Command	Remarks
3. Configure mappings for the priority map.	**import** *import-value-list* **export** *export-value*	By default, the default priority maps are used. For more information, see "Appendixes." Newly configured mappings overwrite the old ones.

Configuring a port to trust packet priority for priority mapping

You can configure the device to trust a particular priority field carried in packets for priority mapping on ports or globally.

When you configure the trusted packet priority type on an interface, use the following available keywords:

- **dot1p**—Uses the 802.1p priority of received packets for mapping.
- **dscp**—Uses the DSCP precedence of received IP packets for mapping.

To configure the trusted packet priority type on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure the trusted packet priority type.	**qos trust** { **dot1p** | **dscp** }	By default, the port priority is trusted.

Changing the port priority of an interface

If an interface does not trust any packet priority, the device uses its port priority to look for priority parameters for the incoming packets. By changing port priority, you can prioritize traffic received on different interfaces.

To change the port priority of an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Set the port priority of the interface.	**qos priority** *priority-value*	The default setting is 0.

Displaying and maintaining priority mapping

Execute **display** commands in any view.

Task	Command
Display priority map configuration.	**display qos map-table** [**dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp**]
Display the trusted packet priority type on a port.	**display qos trust interface** [*interface-type interface-number*]

Priority mapping configuration examples

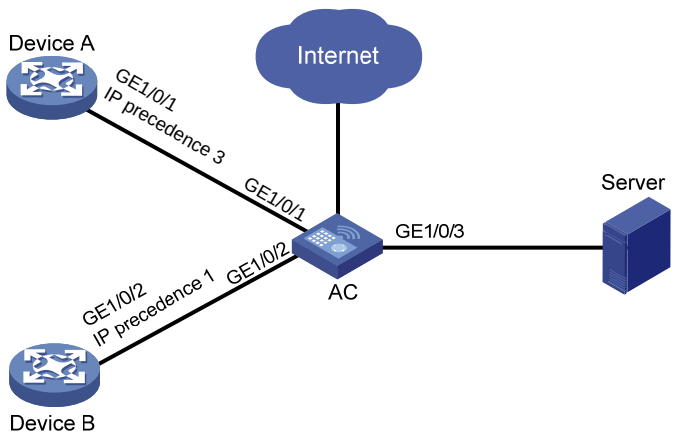
Network requirements

As shown in Figure 4:

- The IP precedence of traffic from Device A to the AC is 3.
- The IP precedence of traffic from Device B to the AC is 1.

Configure the AC to preferentially process packets from Device A to the server when GigabitEthernet 1/0/3 of the AC is congested.

Figure 4 Network diagram



Configuration procedure

Assign port priority to GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2. Make sure the following requirements are met:

- The priority of GigabitEthernet 1/0/1 is higher than that of GigabitEthernet 1/0/2.

- No trusted packet priority type is configured on GigabitEthernet 1/0/1 or GigabitEthernet 1/0/2.

```
<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] qos priority 3
[AC-GigabitEthernet1/0/1] quit
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] qos priority 1
[AC-GigabitEthernet1/0/2] quit
```

Configuring traffic policing

Overview

Traffic policing helps assign network resources (including bandwidth) and increase network performance. For example, you can configure a flow to use only the resources committed to it in a certain time range. This avoids network congestion caused by burst traffic.

Traffic policing controls the traffic rate and resource usage according to traffic specifications. You can use token buckets for evaluating traffic specifications.

Traffic evaluation and token buckets

Token bucket features

A token bucket is analogous to a container that holds a certain number of tokens. Each token represents a certain forwarding capacity. The system puts tokens into the bucket at a constant rate. When the token bucket is full, the extra tokens cause the token bucket to overflow.

Evaluating traffic with the token bucket mechanism

The token bucket mechanism evaluates each packet by looking at the number of tokens in the bucket. If the number of tokens in the bucket is enough for forwarding a packet:

- The packet conforms to the specification (called conforming traffic) and is colored green.
- The corresponding tokens are taken away from the bucket.

Otherwise, the packet does not conform to the specification (called excess traffic) and is colored red.

Traffic policing uses the single rate two color mechanism. This mechanism uses one token bucket (bucket C) and the following parameters:

- **Committed information rate (CIR)**—Mean rate at which tokens are put into bucket C. It sets the average packet transmission or forwarding rate allowed by bucket C.
- **Committed burst size (CBS)**—Size of bucket C, which specifies the transient burst of traffic that bucket C can forward in each burst. The CBS must be greater than the maximum packet size.

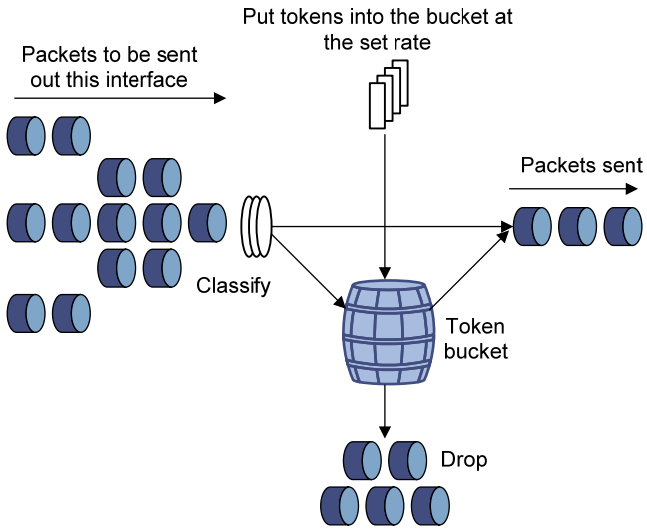
Traffic policing

Traffic policing supports policing the inbound traffic and the outbound traffic.

A typical application of traffic policing is to supervise the specification of traffic entering a network and limit it within a reasonable range. Another application is to "discipline" the extra traffic to prevent aggressive use of network resources by an application. For example, you can limit bandwidth for

HTTP packets to less than 50% of the total. If the traffic of a session exceeds the limit, traffic policing can drop the packets or reset the IP precedence of the packets. Figure 5 shows an example of policing outbound traffic on an interface.

Figure 5 Traffic policing



Traffic policing is widely used in policing traffic entering the ISP networks. It can classify the policed traffic and take predefined policing actions on each packet depending on the evaluation result:

- Forwarding the packet if the evaluation result is "conforming."
- Dropping the packet if the evaluation result is "excess."

Configuration procedure

You can configure traffic policing for an interface only by using the MQC approach. You can configure traffic policing for a user profile by using the MQC approach or non-MQC approach.

Configuring traffic policing by using the MQC approach

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a traffic class and enter traffic class view.	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	By default, no traffic class exists.
3. Configure match criteria.	**if-match** [**not**] *match-criteria*	By default, no match criterion is configured. For more information about the **if-match** command, see *ACL and QoS Command Reference*.
4. Return to system view.	**quit**	N/A

Step	Command	Remarks
5. Create a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*	By default, no traffic behavior exists.
6. Configure a traffic policing action.	**car cir** *committed-information-rate* [**cbs** *committed-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *	By default, no traffic policing action is configured.
7. Return to system view.	**quit**	N/A
8. Create a QoS policy and enter QoS policy view.	**qos policy** *policy-name*	By default, no QoS policy exists.
9. Associate the traffic class with the traffic behavior in the QoS policy.	**classifier** *classifier-name* **behavior** *behavior-name*	By default, a traffic class is not associated with a traffic behavior.
10. Return to system view.	**quit**	N/A
11. Apply the QoS policy.	• Applying the QoS policy to an interface • Applying the QoS policy to a user profile	Choose one of the application destinations as needed. By default, no QoS policy is applied.

Configuring traffic policing for a user profile by using the non-MQC approach

The following matrix shows the feature and hardware compatibility:

Hardware series	Model	Feature compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	No
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes

Hardware series	Model	Feature compatibility
WX5500H series	WX5540H WX5560H WX5580H	Yes
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	Yes

When a user profile is configured, you can perform traffic policing based on users. When any user of the user profile logs in, the authentication server automatically applies the CAR parameters configured for the user profile to the user. When the user logs off, the system automatically removes the CAR configuration without manual intervention.

To configure traffic policing for a user profile:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter user profile view.	**user-profile** *profile-name*	The configuration made in user profile view takes effect when the users are online.
3. Configure a CAR policy for the user profile.	**qos car** { **inbound** | **outbound** } **any cir** *committed-information-rate* [**cbs** *committed-burst-size*]	By default, no CAR policy is configured for a user profile. The conforming traffic is permitted to pass through, and the excess traffic is dropped.

Displaying and maintaining traffic policing

Execute **display** commands in any view.

Task	Command
Display traffic behavior configuration.	**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*] [**slot** *slot-number*]

Configuring traffic filtering

You can filter in or filter out traffic of a class by associating the class with a traffic filtering action. For example, you can filter packets sourced from an IP address according to network status.

Configuration procedure

To configure traffic filtering:

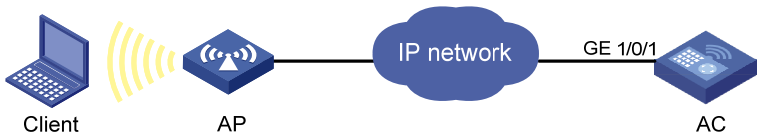
Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a traffic class and enter traffic class view.	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	By default, no traffic class exists.
3. Configure match criteria.	**if-match** [**not**] *match-criteria*	By default, no match criterion is configured.
4. Return to system view.	**quit**	N/A
5. Create a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*	By default, no traffic behavior exists.
6. Configure the traffic filtering action.	**filter** { **deny** | **permit** }	By default, no traffic filtering action is configured.
7. Return to system view.	**quit**	N/A
8. Create a QoS policy and enter QoS policy view.	**qos policy** *policy-name*	By default, no QoS policy exists.
9. Associate the traffic class with the traffic behavior in the QoS policy.	**classifier** *classifier-name* **behavior** *behavior-name*	By default, a traffic class is not associated with a traffic behavior.
10. Return to system view.	**quit**	N/A
11. Apply the QoS policy to an interface.	Applying the QoS policy to an interface	By default, no QoS policy is applied to an interface.
12. (Optional.) Display the traffic filtering configuration.	**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*] [**slot** *slot-number*]	Available in any view.

Configuration example

Network requirements

As shown in Figure 6, configure traffic filtering on GigabitEthernet 1/0/1 to deny the incoming packets with a source port number other than 21.

Figure 6 Network diagram



Configuration procedure

Create advanced ACL 3000, and configure a rule to match packets whose source port number is not 21.

```
<AC> system-view
[AC] acl advanced 3000
[AC-acl-ipv4-adv-3000] rule 0 permit tcp source-port neq 21
[AC-acl-ipv4-adv-3000] quit
```

Create a traffic class named **classifier_1**, and use ACL 3000 as the match criterion in the traffic class.

```
[AC] traffic classifier classifier_1
[AC-classifier-classifier_1] if-match acl 3000
[AC-classifier-classifier_1] quit
```

Create a traffic behavior named **behavior_1**, and configure the traffic filtering action to drop packets.

```
[AC] traffic behavior behavior_1
[AC-behavior-behavior_1] filter deny
[AC-behavior-behavior_1] quit
```

Create a QoS policy named **policy**, and associate traffic class **classifier_1** with traffic behavior **behavior_1** in the QoS policy.

```
[AC] qos policy policy
[AC-qospolicy-policy] classifier classifier_1 behavior behavior_1
[AC-qospolicy-policy] quit
```

Apply the QoS policy named **policy** to the incoming traffic of GigabitEthernet 1/0/1.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] qos apply policy policy inbound
```

Configuring priority marking

Priority marking sets the priority fields or flag bits of packets to modify the priority of packets. For example, you can use priority marking to set the DSCP value for a class of IP packets to control the forwarding of these packets.

To configure priority marking to set the priority fields or flag bits for a class of packets, perform the following tasks:

1. Configure a traffic behavior with a priority marking action.
2. Associate the traffic class with the traffic behavior.

Priority marking can be used together with priority mapping. For more information, see "Configuring priority mapping."

Configuration procedure

To configure priority marking:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a traffic class and enter traffic class view.	**traffic classifier** *classifier-name* [**operator** { **and** | **or** }]	By default, no traffic class exists.
3. Configure match criteria.	**if-match** [**not**] *match-criteria*	By default, no match criterion is configured. For more information about the **if-match** command, see *ACL and QoS Command Reference*.
4. Return to system view.	**quit**	N/A
5. Create a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*	By default, no traffic behavior exists.
6. Configure a priority marking action.	• Set the DSCP value for packets: **remark dscp** *dscp-value* • Set the local precedence for packets: **remark local-precedence** *local-precedence-value*	Use one of the commands. By default, no priority marking action is configured.
7. Return to system view.	**quit**	N/A
8. Create a QoS policy and enter QoS policy view.	**qos policy** *policy-name*	By default, no QoS policy exists.
9. Associate the traffic class with the traffic behavior in the QoS policy.	**classifier** *classifier-name* **behavior** *behavior-name*	By default, a traffic class is not associated with a traffic behavior.

Step	Command	Remarks
10. Return to system view.	**quit**	N/A
11. Apply the QoS policy to an interface.	Applying the QoS policy to an interface	By default, no QoS policy is applied to an interface.
12. (Optional.) Display the priority marking configuration.	**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*] [**slot** *slot-number*]	Available in any view.

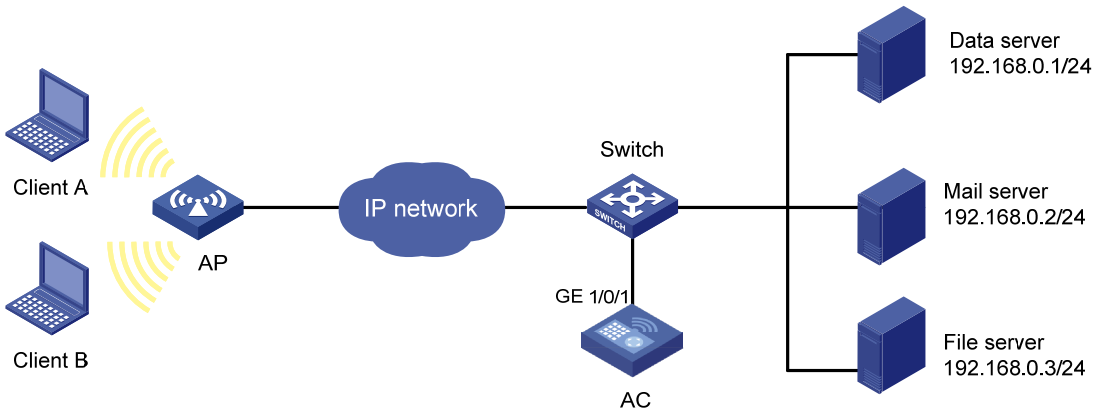
Configuration example

Network requirements

As shown in Figure 7, configure priority marking on the AC to meet the following requirements:

Traffic source	Destination	Processing priority
Client A, B	Data server	High
Client A, B	Mail server	Medium
Client A, B	File server	Low

Figure 7 Network diagram



Configuration procedure

Create advanced ACL 3000, and configure a rule to match packets with destination IP address 192.168.0.1.

```
<AC> system-view
[AC] acl advanced 3000
[AC-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.1 0
[AC-acl-ipv4-adv-3000] quit
```

Create advanced ACL 3001, and configure a rule to match packets with destination IP address 192.168.0.2.

```
[AC] acl advanced 3001
[AC-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.2 0
[AC-acl-ipv4-adv-3001] quit
```

Create advanced ACL 3002, and configure a rule to match packets with destination IP address 192.168.0.3.

```
[AC] acl advanced 3002
[AC-acl-ipv4-adv-3002] rule permit ip destination 192.168.0.3 0
[AC-acl-ipv4-adv-3002] quit
```

Create a traffic class named **classifier_dbserver**, and use ACL 3000 as the match criterion in the traffic class.

```
[AC] traffic classifier classifier_dbserver
[AC-classifier-classifier_dbserver] if-match acl 3000
[AC-classifier-classifier_dbserver] quit
```

Create a traffic class named **classifier_mserver**, and use ACL 3001 as the match criterion in the traffic class.

```
[AC] traffic classifier classifier_mserver
[AC-classifier-classifier_mserver] if-match acl 3001
[AC-classifier-classifier_mserver] quit
```

Create a traffic class named **classifier_fserver**, and use ACL 3002 as the match criterion in the traffic class.

```
[AC] traffic classifier classifier_fserver
[AC-classifier-classifier_fserver] if-match acl 3002
[AC-classifier-classifier_fserver] quit
```

Create a traffic behavior named **behavior_dbserver**, and configure the action of setting the local precedence value to 4.

```
[AC] traffic behavior behavior_dbserver
[AC-behavior-behavior_dbserver] remark local-precedence 4
[AC-behavior-behavior_dbserver] quit
```

Create a traffic behavior named **behavior_mserver**, and configure the action of setting the local precedence value to 3.

```
[AC] traffic behavior behavior_mserver
[AC-behavior-behavior_mserver] remark local-precedence 3
[AC-behavior-behavior_mserver] quit
```

Create a traffic behavior named **behavior_fserver**, and configure the action of setting the local precedence value to 2.

```
[AC] traffic behavior behavior_fserver
[AC-behavior-behavior_fserver] remark local-precedence 2
[AC-behavior-behavior_fserver] quit
```

Create a QoS policy named **policy_server**, and associate traffic classes with traffic behaviors in the QoS policy.

```
[AC] qos policy policy_server
```

```
[AC-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[AC-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[AC-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[AC-qospolicy-policy_server] quit
```

Apply the QoS policy named **policy_server** to the incoming traffic of GigabitEthernet 1/0/1.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] qos apply policy policy_server inbound
[AC-GigabitEthernet1/0/1] quit
```

Appendixes

Appendix A Acronym

Table 1 Appendix A Acronym

Acronym	Full spelling
BE	Best Effort
CAR	Committed Access Rate
CBS	Committed Burst Size
CIR	Committed Information Rate
DiffServ	Differentiated Service
DSCP	Differentiated Services Code Point
EBS	Excess Burst Size
IntServ	Integrated Service
ISP	Internet Service Provider
PIR	Peak Information Rate
QoS	Quality of Service
ToS	Type of Service

Appendix B Default priority maps

Table 2 Default dot1p-lp priority map

Input priority value	dot1p-lp map
dot1p	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Table 3 Default dot11e-lp priority map

dot11e	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Table 4 Default dscp-lp priority map

Input priority value	dscp-lp map
dscp	lp
0 to 7	0
8 to 15	1
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

Table 5 Default lp-dot1p, lp-dot11e, and lp-dscp priority maps

Input priority value	lp-dot1p map	lp-dot11e map	lp-dscp map
lp	dot1p	dot11e	DSCP
0	1	1	0
1	2	2	8
2	0	0	16
3	3	3	24
4	4	4	32
5	5	5	40
6	6	6	48
7	7	7	56

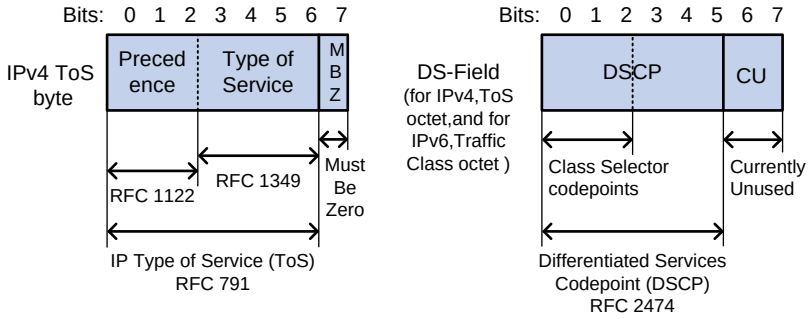
Table 6 Default port priority-local priority map

Port priority	Local precedence
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Appendix C Introduction to packet precedences

IP precedence and DSCP values

Figure 8 ToS and DS fields



As shown in Figure 8, the ToS field in the IP header contains 8 bits. The first 3 bits (0 to 2) represent IP precedence from 0 to 7. According to RFC 2474, the ToS field is redefined as the differentiated services (DS) field. A DSCP value is represented by the first 6 bits (0 to 5) of the DS field and is in the range 0 to 63. The remaining 2 bits (6 and 7) are reserved.

Table 7 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

IP precedence (decimal)	IP precedence (binary)	Description
6	110	internet
7	111	network

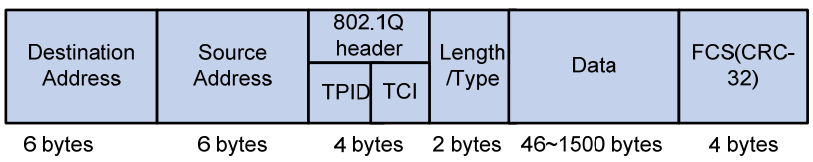
Table 8 DSCP values

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)

802.1p priority

802.1p priority lies in the Layer 2 header. It applies to occasions where Layer 3 header analysis is not needed and QoS must be assured at Layer 2.

Figure 9 An Ethernet frame with an 802.1Q tag header



As shown in Figure 9, the 4-byte 802.1Q tag header contains the 2-byte tag protocol identifier (TPID) and the 2-byte tag control information (TCI). The value of the TPID is 0x8100. Figure 10 shows the format of the 802.1Q tag header. The Priority field in the 802.1Q tag header is called 802.1p priority, because its use is defined in IEEE 802.1p. Table 9 shows the values for 802.1p priority.

Figure 10 802.1Q tag header

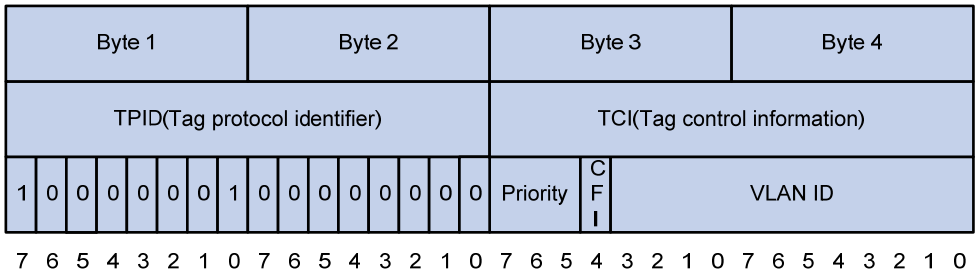


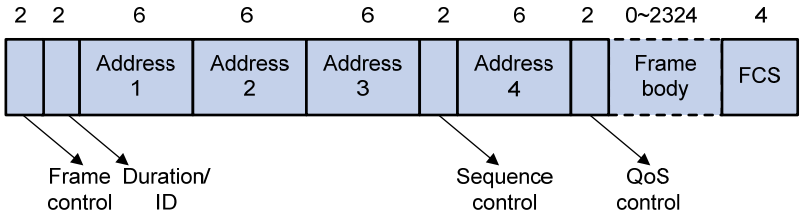
Table 9 Description on 802.1p priority

802.1p priority (decimal)	802.1p priority (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

802.11e priority

To provide QoS services on WLAN, the 802.11e standard was developed. IEEE 802.11e is a MAC-layer enhancement to IEEE 802.11. IEEE 802.11e adds a 2-byte QoS control field to the 802.11e MAC frame header. The 3-bit QoS control field represents the 802.11e priority in the range of 0 to 7.

Figure 11 802.11e frame structure



Contents

Configuring time ranges

You can implement a service based on the time of the day by applying a time range to it. A time-based service takes effect only in time periods specified by the time range. For example, you can implement time-based ACL rules by applying a time range to them. If a time range does not exist, the service based on the time range does not take effect.

The following basic types of time ranges are available:

- **Periodic time range**—Recurs periodically on a day or days of the week.
- **Absolute time range**—Represents only a period of time and does not recur.

A time range is uniquely identified by the time range name. You can create a maximum of 1024 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements. The active period of a time range is calculated as follows:

1. Combining all periodic statements.
2. Combining all absolute statements.
3. Taking the intersection of the two statement sets as the active period of the time range.

Feature and hardware compatibility

Hardware series	Model	Time range compatibility
WX1800H series	WX1804H WX1810H WX1820H	Yes
WX2500H series	WX2510H WX2540H WX2560H	Yes
WX3000H series	WX3010H WX3010H-L WX3010H-X WX3024H WX3024H-L	Yes: • WX3010H • WX3010H-X • WX3024H No: • WX3010H-L • WX3024H-L
WX3500H series	WX3508H WX3510H WX3520H WX3540H	Yes
WX5500E series	WX5510E WX5540E	Yes
WX5500H series	WX5540H WX5560H	Yes

Hardware series	Model	Time range compatibility
	WX5580H	
Access controller modules	EWPXM1MAC0F EWPXM1WCME0 EWPXM2WCMD0F LSQM1WCMX20 LSQM1WCMX40 LSUM1WCME0 LSUM1WCMX20RT LSUM1WCMX40RT	Yes

Configuration procedure

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create or edit a time range.	**time-range** *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }	No time range exists.

Displaying and maintaining time ranges

Execute the **display** command in any view.

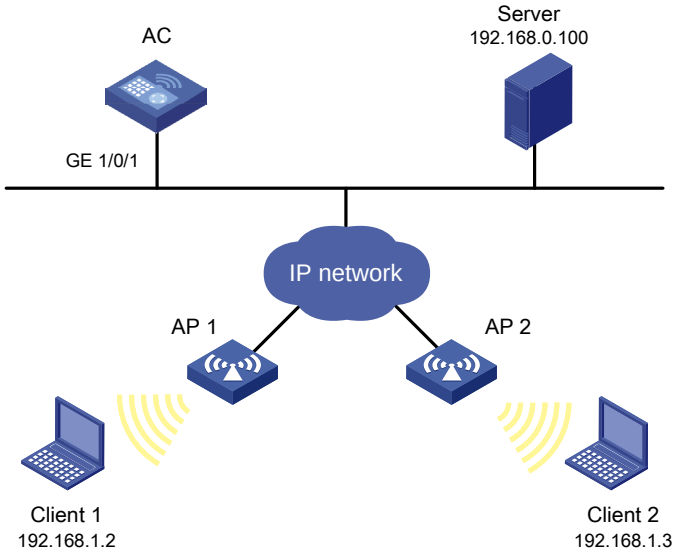
Task	Command
Display time range configuration and status.	**display time-range** { *time-range-name* | **all** }

Time range configuration example

Network requirements

As shown in Figure 1, configure an ACL on the AC to allow Client 1 to access the server only from 8:00 to 18:00 on working days from June 2015 to the end of the year.

Figure 1 Network diagram



Configuration procedure

Create a periodic time range from 8:00 to 18:00 on working days from June 2015 to the end of the year.

```
<AC> system-view
[AC] time-range work 8:0 to 18:0 working-day from 0:0 6/1/2015 to 24:0 12/31/2015
```

Create an IPv4 basic ACL numbered 2001, and configure a rule in the ACL to permit packets only from 192.168.1.2/32 during the time range **work**.

```
[AC] acl basic 2001
[AC-acl-ipv4-basic-2001] rule permit source 192.168.1.2 0 time-range work
[AC-acl-ipv4-basic-2001] rule deny source any time-range work
[AC-acl-ipv4-basic-2001] quit
```

Apply IPv4 basic ACL 2001 to filter outgoing packets on interface GigabitEthernet 1/0/1.

```
[AC] interface gigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1] packet-filter 2001 outbound
[AC-GigabitEthernet1/0/1] quit
```

Verifying the configuration

Display time range configuration and status on the AC.

```
[AC] display time-range all
Current time is 09:40:55 5/26/2015 Tuesday

Time-range : work ( Active )
 08:00 to 18:00 working-day
 from 00:00 6/1/2011 to 00:00 1/1/2012
```

The output shows that the time range **work** is active.