
Contents

1 Configuring ACL.....	1
1.1 Introduction.....	1
1.1.1 Overview.....	1
1.1.2 Principles.....	1
1.2 Configuration Task Summary.....	14
1.3 Configuring an IP Standard ACL.....	14
1.3.1 Overview.....	14
1.3.2 Restrictions and Guidelines.....	14
1.3.3 Configuration Tasks.....	14
1.3.4 Creating an IP Standard ACL.....	15
1.3.5 Applying an IP Standard ACL.....	16
1.3.6 Configuring a Global Security ACL.....	17
1.3.7 Configuring a Security Channel.....	18
1.3.8 Configuring a Redirect ACL.....	19
1.3.9 Configuring the Fragmented Packet Matching Mode.....	20
1.3.10 Configuring the SVI Router ACL.....	20
1.4 Configuring an IP Extended ACL.....	21
1.4.1 Overview.....	21
1.4.2 Restrictions and Guidelines.....	21
1.4.3 Configuration Tasks.....	21
1.4.4 Creating an IP Extended ACL.....	21
1.4.5 Applying an IP Extended ACL.....	23
1.4.6 Configuring a Global Security ACL.....	24

1.4.7 Configuring a Security Channel.....	25
1.4.8 Configuring a Redirect ACL.....	26
1.4.9 Configuring the Fragmented Packet Matching Mode.....	27
1.4.10 Configuring the SVI Router ACL.....	27
1.5 Configuring a MAC Extended ACL.....	28
1.5.1 Overview.....	28
1.5.2 Restrictions and Guidelines.....	28
1.5.3 Configuration Tasks.....	28
1.5.4 Creating a MAC Extended ACL.....	28
1.5.5 Applying a MAC Extended ACL.....	29
1.5.6 Configuring a Security Channel.....	30
1.5.7 Configuring a Redirect ACL.....	31
1.5.8 Configuring the SVI Router ACL.....	32
1.6 Configuring an Expert Extended ACL.....	33
1.6.1 Overview.....	33
1.6.2 Restrictions and Guidelines.....	33
1.6.3 Configuration Tasks.....	33
1.6.4 Creating an Expert Extended ACL.....	33
1.6.5 Applying an Expert Extended ACL.....	35
1.6.6 Configuring a Global Security ACL.....	36
1.6.7 Configuring a Security Channel.....	36
1.6.8 Configuring a Redirect ACL.....	37
1.6.9 Configuring the Fragmented Packet Matching Mode.....	38
1.6.10 Configuring the SVI Router ACL.....	38

1.7 Configuring an IPv6 ACL.....	39
1.7.1 Overview.....	39
1.7.2 Restrictions and Guidelines.....	39
1.7.3 Configuration Tasks.....	39
1.7.4 Creating an IPv6 ACL.....	39
1.7.5 Applying an IPv6 ACL.....	41
1.7.6 Configuring a Global Security ACL.....	42
1.7.7 Configuring a Security Channel.....	43
1.7.8 Configuring a Redirect ACL.....	44
1.7.9 Configuring the SVI Router ACL.....	44
1.8 Configuring an Expert Advanced ACL (ACL80).....	45
1.8.1 Overview.....	45
1.8.2 Restrictions and Guidelines.....	45
1.8.3 Configuration Tasks.....	45
1.8.4 Creating an ACL80.....	45
1.8.5 Applying an ACL80.....	46
1.8.6 Configuring the SVI Router ACL.....	47
1.9 Monitoring.....	47
1.10 Examples.....	48
1.10.1 Configuring an IP Standard ACL.....	48
1.10.2 Configuring an IP Extended ACL.....	50
1.10.3 Configuring a MAC Extended ACL.....	55
1.10.4 Configuring an Expert Extended ACL.....	57
1.10.5 Configuring an IPv6 ACL.....	60

1.10.6 Configuring an ACL80.....	61
1.10.7 Configuring a Global Security ACL.....	64
1.10.8 Configuring ACL Rules Based on Time Range.....	66

1 Configuring ACL

1.1 Introduction

1.1.1 Overview

The access control list (ACL) is also called access list or packet filtering in some documents. An ACL defines a series of "permit" or "deny" rule statements, and applies these rules to a device interface to control the data packets entering/leaving the interface, so as to improve the security of network devices.

Configuring ACL can guarantee network security, reliability, and stability, for example:

- Preventing packet attacks: An ACL can be configured to deny the attacks launched using the Internet Protocol (IP), Transmission Control Protocol (TCP), or Internet Control Message Protocol (ICMP) packets.
- Controlling network access: An ACL can be configured to restrict users to some services, for example, users are allowed to access only the WWW and email services, but not allowed to access other services such as telnet; some users are allowed to access services only within a given time period, or only certain hosts are allowed to access the network.
- Controlling network traffic: An ACL can be used together with quality of service (QoS) to guarantee prioritized services for some important data flows. For QoS configuration, see "Configuring QoS."

1.1.2 Principles

1. Basic Concepts

- ACL

ACLs are classified into basic ACLs and dynamic ACLs.

Users can select a basic ACL or a dynamic ACL as needed. In general, a basic ACL can meet security requirements. However, experienced hackers may counterfeit source addresses by using some software to spoof devices and access the network. Before users access the network, the dynamic ACL requires them to pass identity authentication, which makes it hard for hackers to attack the network. Therefore, the dynamic ACL can be used in some sensitive areas to ensure network security.

Note

Spoofing devices by counterfeiting source addresses, namely, spoofing, is an inherent problem of all ACLs. Spoofing also occur on the dynamic ACL: Hackers may fake users' addresses to access the network during the effective access period after the users pass the identity authentication. This problem can be solved in two ways. One is to set the idle time of user access to a smaller value so that it is more difficult for hackers to break into the network. The other is to use the IP Security (IPSec) encryption protocol to encrypt the network data, and ensure that all the data is encrypted when the data is transmitted to a device.

The ACL is generally configured on the following network devices:

- A device between an internal network and an external network (such as the Internet)
- A device at the boundary of two parts of the network
- A device connecting to a control port
- ACE

An access control entry (ACE) is a statement containing the "permit" or "deny" action and filtering rules. Each ACE has a sequence number, which is automatically allocated by the device or manually configured. An ACL contains one or more ACEs. The ACL identifies and filters packets by using ACEs.

The sequence of ACEs in an ACL determines the matching priority of the ACEs in the ACL. When processing packets, a network device performs rule matching in the ascending order of ACE sequence numbers. When finding a matched ACE, the network device stops matching subsequent ACEs.

For example, create ACE 10 to deny all data flows.

```
10 deny ip any any
20 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

Since ACE 10 denies all the IP packets, the telnet packet from the host in the 192.168.12.0/24 network is denied even if it matches ACE 20. The reason is that, after finding that the packet matches the first ACE, the device stops matching the packet with the subsequent ACE 20.

Here is another example: Create ACE 10 to permit all IPv6 data flows to pass through.

```
10 permit ipv6 any any
20 deny ipv6 host 200::1 any
```

Since ACE 10 permits all IPv6 packets to pass through, the IPv6 packet sent from the host with IP address 200::1 can pass through even if it matches ACE 20. The reason is that, after finding that the packet matches the first ACE, the device stops matching the packet with the subsequent ACE 20.

- Step

When the device automatically allocates sequence numbers to ACEs, the difference between two adjacent ACE sequence numbers is called a step. For example, if the step is set to 5, the device automatically allocates sequence numbers to ACEs in the ascending order of 5, 10, 15.... See the example below.

```
5 deny ip any any
10 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

After the step is changed, the ACE sequence numbers will be automatically rearranged based on the new step value. For example, when the step is changed to 10, the original ACE sequence numbers are changed from 5, 10, and 15 to 5, 15, and 25.

A new ACE can be inserted between two ACEs by changing the step. For example, four ACEs are created, and the ACEs are manually numbered 1, 2, 3, and 4 in turn. To insert a new ACE after ACE 1, first change the step to 2 (then, the sequence numbers of the original four ACEs automatically change to 1, 3, 5, and 7), and then insert a manually configured ACE with sequence number 2.

- Filter field template

Filter fields mean the fields used to identify and classify packets when an ACE is generated. A filter field template is a combination of such fields. An ACE identifies Ethernet packets by some fields in them, including:

L2 fields:

- o 48-bit source MAC address (the 48-bit source MAC address must be matched completely)
- o 48-bit destination MAC address (the 48-bit destination MAC address must be matched completely)
- o 16-bit L2 type field

L3 fields:

- o Source IP address field (all the source IP address values can be matched or a subnet can be used to define a type of flow)
- o Destination IP address field (all the destination IP address values can be matched or a subnet can be used to define a type of flow)
- o Protocol type field

L4 fields:

- o You can define a TCP source port, destination port, or both for matching; you can also define the range of the source port or destination port for matching.
- o You can define a User Datagram Protocol (UDP) source port, destination port, or both for matching; you can also define the range of the source port or destination port for matching.

For example, you can create an ACE to identify and classify packets based on their destination IP address field. You can also create another ACE to identify and classify packets based on their source IP address field and UDP source port field. These two ACEs use different filter field templates.

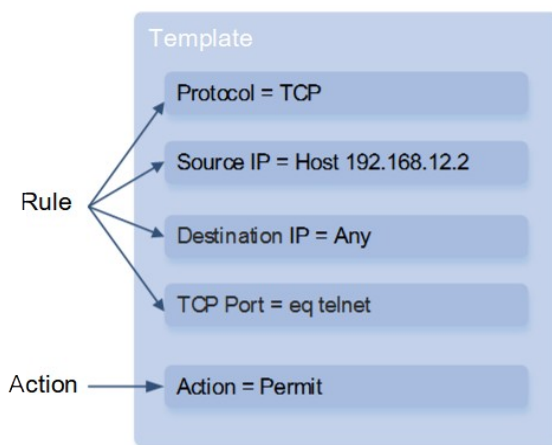
● Rules

Rules refer to the values of fields in an ACE filter field template. For example, an ACE reads as follows:

```
10 permit tcp host 192.168.12.2 any eq telnet
```

In this ACE, the filter field template is a collection of the following fields: source IP address field, destination IP address field, IP protocol field, and TCP destination port field. The corresponding values (namely, rules) are as follows: The source IP address is **Host 192.168.12.2**, the destination IP address is **Any** (namely, all the hosts), the IP protocol is **TCP**, and the TCP destination port is **Telnet**. See Figure 1-1.

Figure 1-1 Analysis of ACE: permit tcp host 192.168.12.2 any eq telnet



Note

- A filter field template can be a collection of L3 fields and L4 fields, or a collection of multiple L2 fields. However, the filter field templates of the standard and extended ACLs cannot be a collection of L2 and L3 fields, or L2 and L4 fields, or L2, L3, and L4 fields. To use a collection of L2, L3, and L4 fields, you can use an expert extended ACL.
- Outbound ACLs to be associated with switch virtual interfaces (SVIs) can be IP standard, IP extended, MAC extended, or expert ACLs.
- If a destination MAC address is configured for matching in MAC extended and expert ACLs and such ACLs are applied in the outbound direction of an SVI, the ACEs containing the destination MAC address can be configured but fail to take effect. If you configure a destination IP address for matching in the IP extended and expert ACLs but the destination IP address is not within the subnet IP address range of the associated SVI, the configured ACLs do not take effect. For example, if VLAN 1 has an IP address 192.168.64.1 255.255.255.0 and an IP extended ACL is created, with the ACE **deny udp any 192.168.65.1 0.0.0.255 eq 255**, this ACL does not take effect when it is applied to the egress of VLAN 1. The cause is that the destination IP address is not within the subnet IP address range of VLAN 1. If the ACE is **deny udp any 192.168.64.1 0.0.0.255 eq 255**, the ACL takes effect because the destination IP address complies with the requirements.

Note

- When an expert ACL is configured and applied to the outbound direction of a port, if some ACEs in the ACL contain L3 matching information (such as IP address and L4 port), the non-IP packets received by the port cannot be subjected to the permit and deny ACEs of the ACL.

2. IP ACL

IP ACL implements refined control over the IPv4 packets entering/leaving the device. You can deny or permit specific IPv4 packets destined to a network according to the actual needs, so as to control the access of IP users to network resources.

You can define a series of access rules in an IP ACL, and apply the ACL to the inbound or outbound direction of a port. You can also apply an IP ACL globally. When IPv4 packets enter or leave a device, the device determines whether to forward or block them by judging whether they match the rules.

To configure an IP ACL on a device, you must specify a unique name or number for each ACL to uniquely identify the ACL.

IP ACLs are classified into IP standard ACLs and IP extended ACLs. Table 1-1 lists the ranges of numbers that can be used for IP standard ACLs and IP extended ACLs.

Table 1-1 Number Ranges for IP Standard ACLs and IP Extended ACLs

Type	Number Range	Matching Field
IP standard ACL	1 to 99, 1300 to 1999	Source IP address

Type	Number Range	Matching Field
IP extended ACL	100 to 199, 2000 to 2699	<ul style="list-style-type: none"> ● Source IP address ● Destination IP address ● IP protocol number ● L4 source port ID or ICMP type ● L4 destination port ID or ICMP code

The IP standard ACL controls the forwarding or blocking of packets based on the source IP address. The IP extended ACL controls the forwarding or blocking of packets by combining the matching fields in the table above.

A single ACL can use multiple independent ACL statements to define multiple rules, and all the statements use the same number or name so that the statements are bound to the same ACL.

Note

On routers, the ICMP code matching field in ACL rules is invalid for the ICMP packets with ICMP type 3. If the code field for matching ICMP packets is configured in an ACL rule, when ACL matching is performed on the ICMP packets with type 3 on the routers, the matching result may be different from the expected result.

One rule statement of denying all data flows is hidden at the end of each IP ACL. If a packet fails to match any rules, it will be denied. For example:

```
access-list 1 permit host 192.168.4.12
```

This ACL only permits the packets with source host address 192.168.4.12 to pass through, and denies the packets of the other hosts. The reason is that this ACL contains a rule statement at its end as follows:

```
access-list 1 deny any
```

Here is another example:

```
access-list 1 deny host 192.168.4.12
```

If an ACL contains the above statement only, the packets of all the hosts are denied when passing through the port.

Warning

When defining an ACL, you must consider the route update packets. The rule statement of denying all data flows at the end of the ACL may result in blocking of all the route update packets.

The reflexive ACL automatically generates a temporary ACL according to the L3 and L4 information of the traffic originated from the internal network. A temporary ACL is created according to the following principles: The IP protocol number remains unchanged, the source IP address and destination IP address are strictly interchanged, and the TCP/UDP source port and destination port are strictly interchanged. Only when the L3 and L4 information of the returned traffic strictly matches that in the temporary ACL previously created based on the outbound traffic, will the device permit the traffic to enter the internal network.

3. MAC Extended ACL

The MAC extended ACL implements refined control over the packets entering/leaving the device based on the L2 information of the packets. You can deny or permit specific L2 packets destined to a network according to the actual needs, so as to protect network resources against attacks or control the access of users to network resources.

You can define a series of access rules in a MAC extended ACL, and apply the ACL to the inbound or outbound direction of a port. When packets enter or leave a device, the device determines whether to forward or block them by judging whether they match the rules.

To configure a MAC extended ACL on a device, you must specify a unique name or number for each ACL to uniquely identify the ACL. Table 1-1 lists the range of numbers for the MAC extended ACLs.

Table 1-1 Number Range for MAC Extended ACLs

Type	Number Range	Matching Field
MAC extended ACL	700 to 799	<ul style="list-style-type: none"> ● Source MAC address ● Destination MAC address ● Ethernet protocol type

The MAC extended ACL controls the forwarding or blocking of packets based on the source or destination MAC address and the Ethernet type of packets.

A single MAC extended ACL can use multiple independent ACL statements to define multiple rules, and all the statements use the same number or name so that the statements are bound to the same ACL.

Note

If a MAC extended ACL rule does not specify IPv6 packets, that is, the Ethernet type field is not defined or the defined Ethernet type field value is not 0x86dd, then the MAC extended ACL is not used to match IPv6 packets. If you need to match IPv6 packets, define an IPv6 ACL.

One rule statement of denying all data flows is hidden at the end of each MAC extended ACL. If a packet fails to match any rules, it will be denied. For example:

```
access-list 700 permit host 00d0.f800.0001 any
```

This ACL permits only the packets sent from the host with MAC address 00d0.f800.0001 to pass through, and denies the packets from all the other hosts. The reason is that this ACL contains a rule statement at its end as follows:

```
access-list 700 deny any any
```

4. Expert Extended ACL

The expert extended ACL is also known as expert-level extended ACL. The expert extended ACL implements refined control over the packets entering/leaving a device based on the L2 and L3 information of the packets. The expert extended ACL can be regarded as a combination and enhancement of the IP ACL and MAC

extended ACL. An expert extended ACL can contain IP ACL rules and MAC extended ACL rules, and specify VLAN IDs for packet matching.

You can define a series of access rules in an expert extended ACL, and apply the ACL to the inbound or outbound direction of a port. When packets enter or leave a device, the device determines whether to forward or block them by judging whether they match the access rules.

To configure an expert extended ACL on a device, you must specify a unique name or number for each ACL to uniquely identify the ACL. Table 1-1 lists the range of numbers that can be used for expert extended ACLs.

Table 1-1 Number Range for Expert Extended ACLs

Type	Number Range	Matching Field
Expert extended ACL	2700 to 2899	<ul style="list-style-type: none"> ● Source IP address ● Destination IP address ● IP protocol number ● L4 source port ID or ICMP type ● L4 destination port ID or ICMP code ● Source MAC address ● Destination MAC address ● Ethernet protocol type ● VLAN ID

The expert extended ACL controls the forwarding or blocking of packets by combining the matching fields in the table above.

A single expert extended ACL can use multiple independent ACL statements to define multiple rules, and all the statements must use the same number or name so that the statements are bound to the same ACL.

One rule statement of denying all data flows is hidden at the end of each expert extended ACL. If a packet fails to match any rules, it will be denied. For example:

```
access-list 2700 permit 0x0806 any any any any any
```

This ACL only permits the packets with Ethernet type 0x0806 (namely, ARP) to pass through, and denies the packets of the other types. The reason is that this ACL contains a rule statement at its end as follows:

```
access-list 2700 deny any any any any
```

5. IPv6 ACL

The IPv6 ACL implements refined control over the IPv6 packets entering/leaving a device. You can deny or permit specific IPv6 packets destined to a network according to the actual needs, so as to control the access of IPv6 users to network resources.

You can define a series of access rules in an IPv6 ACL, and apply the ACL to the inbound or outbound direction of a port. When IPv6 packets enter or leave a device, the device determines whether to forward or block them by judging whether they match the rules.

To configure an ACL on a device, you must specify a unique name for the ACL of a protocol.

Note

- Different from IP ACLs, MAC extended ACLs, and expert extended ACLs, an IPv6 ACL must have the name rather than the number specified during creation.
- Only one IP ACL, one MAC extended ACL, or one expert extended ACL can be applied to the inbound or outbound direction of a device port. Besides, an IPv6 ACL can be applied.

One rule statement of denying all IPv6 data flows is hidden at the end of each IPv6 ACL. If a packet fails to match any rules, it is denied. For example:

```
ipv6 access-list ipv6_acl
10 permit ipv6 host 200::1 any
```

This ACL only permits the IPv6 packets coming from source host 200::1 to pass through, and denies the IPv6 packets from all the other hosts. The reason is that this ACL contains a rule statement at its end as follows:

```
deny ipv6 any any
```

Warning

Although each IPv6 ACL contains the rule statement of denying all the IPv6 packets by default, it does not deny neighbor discovery (ND) packets.

6. ACL80

ACL80 is the expert advanced ACL, also known as user-defined ACL. ACL80 supports matching the specified bytes in the first 80 bytes of a packet by bit.

There are three elements in ACL80 matching: matching field content, matching field mask, and the start position (that is, the offset) of matching. The bits of the matching field content map to those of the matching field mask. The matching field content specifies the field value to be matched, and the matching field mask specifies whether the corresponding bits need to be matched. When a bit needs to be matched, the corresponding bit in the matching field mask must be set to **1**. If a bit in a matching field mask is set to **0**, the corresponding bit in the matching field content will not be matched regardless of the bit value in the matching field content. For example:

```
10 permit 00d0f8123456 ffffffff 0
20 deny 00d0f8654321 ffffffff 6
```

In ACE 10, the matching field content is 00d0f8123456, the matching field mask is ffffffff, and the offset is 0. This rule indicates that, if the destination MAC address of a packet is 00d0f8123456, the packet is permitted to be forwarded.

In ACE 20, the matching field content is 00d0f8654321, the matching field mask is ffffffff, and the offset is 6. This rule indicates that, if the source MAC address of a packet is 00d0f8654321, the packet is blocked.

You need to deeply understand the L2 data frame structure so as to use the user-defined ACL correctly. Figure 1-1 shows the first 64 bytes of an L2 data frame. In the figure, each letter represents one hexadecimal number and every two letters represent one byte.

Figure 1-1 First 64 Bytes of an L2 Data Frame

AA	AA	AA	AA	AA	AA	BB	BB	BB	BB	BB	BB	CC	CC	DD	DD
DD	DD	EE	FF	GG	HH	HH	HH	II	II	JJ	KK	LL	LL	MM	MM
NN	NN	OO	PP	QQ	QQ	RR	RR	RR	RR	SS	SS	SS	SS	TT	TT
UU	UU	VV	VV	VV	VV	ww	ww	ww	ww	XY	ZZ	aa	aa	bb	bb

Table 1-1 lists the meaning and offset value of each letter.

Table 1-1 Meanings and Offset Values of Letters

Letter	Description	Offset	Letter	Description	Offset
A	Destination MAC address	0	O	TTL field	34
B	Source MAC address	6	P	Protocol number	35
C	VLAN tag field	12	Q	IP checksum	36
D	Data frame length field	16	R	Source IP address	38
E	Destination service access point (DSAP) field	18	S	Destination IP address	42
F	Source service access point (SSAP) field	19	T	TCP source port	46
G	Control field	20	U	TCP destination port	48
H	Org code field	21	V	Serial number	50
I	Encapsulated data type	24	W	Acknowledgment field	54
J	IP version No.	26	XY	IP header length and reserved bits	58
K	ToS field	27	Z	Reserved bits and flags bits	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

The offset of each field in the table is their offset in the IEEE 802.3 data frame containing the SNAP+Tag fields. The user-defined ACL extracts specific fields from the first 80 bytes of a data frame according to offsets listed in Table 1-5, and then compare the fields with the matching field masks so as to determine the matching field

content. For example, if you permit all TCP packets to be forwarded, you can set the matching field content to **06**, the matching field mask to **ff**, and the offset to **35**. Create ACE 10 as follows:

```
10 permit 06 ff 35
```

Apply the ACL to the inbound or outbound direction of a port. When a packet enters or leaves a device, ACL80 extracts the content of the TCP protocol number field from the data frame, and then compares the content with the matching field content to find out all the matched TCP packets for forwarding.

Note

- ACL80 supports matching Ethernet packets, IEEE 802.3 SNAP packets, and IEEE 802.3 LLC packets. If the values of the **DSAP** field to the **Control** field to be matched are **AAAA03**, the IEEE 802.3 SNAP packets need to be matched. If the values of the **DSAP** field to the **Control** field to be matched are **E0E003**, the 802.3 LLC packets need to be matched. You cannot set the matching of these fields for Ethernet packets.
 - Due to hardware reasons, currently ACL80 cannot implement random byte matching for the first 80 bytes of packets, but only supports matching the locations of the destination MAC address, source MAC address, VLAN ID, ETYPE, IP protocol number, source IPv4 address, destination IPv4 address, source port, destination port, ICMP_TYPE, ICMP_CODE, and PPPOE_IPTYPE fields in packets.
 - When an ACL80 is used to match IP, ARP, and other information, the encapsulated data type and data type mask need to be configured first, that is, the field with offset 24 needs to be configured first, and the mask needs to be set to all Fs. For example, to allow the packets with the source IP address 192.168.1.2 to pass through, the corresponding configuration command is **permit 0800 FFFF 24 C0A80102 FFFFFFFF 38**.
-

7. Redirect ACL

Redirect ACL enables a device to analyze a received packet and redirect it to a specified port for forwarding. To analyze specific packets entering the device, you can configure the redirect ACL function to redirect the packets conforming to the rules to a specified port, which captures the packets for analysis.

Redirect ACL binds an ACL on an input port and specifies an output port. When the input port receives a packet, it queries ACL rules bound to the port one by one. If the packet conforms to the characteristics described in a rule, it is forwarded from the output port specified by the policy.

Note

- Redirect ACL takes effect only in the inbound direction of a port
 - Only one global redirect ACL can be configured.
 - When the global redirect ACL is configured with the destination port, the port is not affected by the global redirect ACL.
-

8. Global Security ACL

There are various virus packets in the network, and the identification characteristics of virus packets are the same or similar on each port. You can create an ACL, add ACEs that match the characteristics of various virus packets, and apply the ACL to each port of a device to filter out virus packets. Such an ACL is called port-based security ACL. In consideration of secure deployment, a port-based security ACL is often configured to filter out packets that comply with some characteristics (such as forged TCP attack packets) and prevent virus packets.

When the port-based security ACL is used in the attack-defense scenarios such as virus filtering, there are much inconvenience.

- Ports must be configured one by one. Duplicate configuration, poor operating performance, and excessive consumption of ACL resources can occur.
- The access control function of the security ACL is weakened. Because the security ACL is used for virus filtering, the basic functions of the security ACL including restricting route updates and restricting network access become unavailable.

The global security ACL can be used for global anti-virus deployment and defense without affecting the port-based security ACL. A global security ACL can take effect on all the L2 ports after one command is configured.

When both the global security ACL and port-based security ACL are configured, they take effect at the same time. The packets that match rules in the global security ACL will be directly filtered out as virus packets, and the packets that fail to match the rules of the global security ACL are still controlled by the port-based security ACL. To exempt some ports from the control of the global security ACL, disable the global security ACL function on these ports. When the global, port-based, and VLAN-based security ACLs are applied at the same time, the priority is port-based security ACL, VLAN-based security ACL, and global security ACL in the descending order.

To avoid misconfiguration of the global security ACL, the global security ACL disabling function is provided. If you disable the global security ACL function and then configure a global security ACL, the system prompts a configuration failure. If you have configured a global security ACL and then disable the global security ACL function, the system deletes all the current global security ACLs and displays a log prompt.

Note

- Since the global security ACL is mainly used for virus filtering, among the ACEs in a global security ACL, only the deny ACEs are installed and take effect, and the permit ACEs will not take effect.
 - Different from a security ACL applied to a port, a global security ACL has no default rule statement of denying all data flows, that is, packets not matching the rules in a global security ACL can pass through.
 - A global security ACL can take effect on both L2 ports and L3 ports. That is, it can take effect on the following types of ports: access port, trunk port, hybrid port, L3 Ethernet port, L2 or L3 aggregation port. It does not take effect on SVIs.
 - You can disable the global security ACL independently on physical ports and L2 or L3 aggregation ports, but not on the member ports of an aggregation port.
 - Global security ACLs can be associated only with IP standard ACLs, IP extended ACLs, MAC extended ACLs, and expert extended ACLs.
-

9. Security Channel

In some application scenarios, the packets complying with certain characteristics must bypass the check of access control application. For example, before the IEEE 802.1x authentication, users must be allowed to log in to the specified resource site and download the IEEE 802.1x authentication client.

This can be achieved through the security channel. A security channel is also an ACL, which can be configured globally or on ports. Applying a security ACL globally or to a port by using a security channel configuration command means that the ACL is a security channel.

When entering a device port, a packet is first checked by the security channel. If the packet meets the matching conditions of the security channel, it bypasses the access control such as port security, Web

authentication, IEEE 802.1x, and IP + MAC binding check, and directly enters the device. The security channel applied globally takes effect for all the non-excluded ports.

Note

- The deny behavior in an ACL applied as a security channel does not take effect, and there is no rule statement of denying all data flows hidden at the end. If a packet does not meet the matching conditions of a security channel, it goes through the check of access control according to the process.
 - You can set up to eight excluded ports for the global security channel, and no port-based security channel can be configured on the excluded ports of the global security channel.
 - When both the port-based authentication migration mode and security channel are used, the security channel does not take effect.
 - You cannot configure an IPv6 ACL as a security channel.
-

10. SVI Router ACL

An ACL applied to an SVI (namely, SVI ACL) takes effect for both the packets forwarded on L2 in a VLAN and the inter-VLAN routed packets. As a result, different users in the same VLAN cannot make normal communication. The SVI router ACL function enables the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

The SVI router ACL function is disabled by default. The SVI ACL takes effect for the inter-VLAN L3 forwarded packets and the intra-VLAN packets forwarded by bridges. After the SVI router ACL function is enabled, the SVI ACL is effective only for the inter-VLAN L3 forwarded packets.

11. Packet Matching Logging

The packet matching logging is used to monitor the running status of ACL rules and provide necessary information for routine network maintenance and network optimization.

To better grasp the running status of ACL in the device, when adding ACEs, you can decide whether to specify the packet matching logging option as needed. If this option is specified, the matching logs are output when ACEs match packets. ACL prints log information based on ACE, that is, the device periodically prints the ACEs that match packets and the number of matched packets. See the example below:

```
*Sep 9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78
packets.
```

To reasonably control the quantity and frequency of log output, ACL allows configuring the log output interval.

Warning

An ACL rule with the log option uses more hardware resources. If all the configured rules have the log option, the hardware policy capacity of the device is halved.

Caution

- The default output interval of packet matching logs is 0 minutes, that is, no ACL matching log is output. After specifying the log option when configuring ACL rules, you also need to configure the output interval, otherwise no matching log is output.
 - For a rule with the log option, if no packet matches the rule within the specified time interval, no packet matching log related to the rule is output; if a packet matches the rule within the specified time interval, the packet matching log related to the rule is output after the time interval expires. The number of
-

matched packets is the total number of packets matching the rule within the time interval, that is, the number of matched packets from the last log output to the current log output.

12. Packet Matching Counting

For the needs of network management, you may want to know whether an ACL rule matches packets and the number of matched packets. ACL provides the rule-based packet matching counting function. You can enable or disable the packet matching counting function for all the rules in an ACL. When a packet matches a rule, the corresponding matching count increases accordingly. You can run the statistics clearing command for an ACL to clear the packet matching counts of all rules in the ACL and start new counting.

Warning

Enabling the packet matching counting function of ACL requires more hardware entries, and in extreme cases, halves the available hardware policy capacity of the device.

13. ACL Effective Time Range

If you need to control some flows within a specified time range, for example, disable chat tools during working hours, you can configure effective time ranges for ACEs to control the pass-through time of flows. The time ranges are classified into absolute time ranges and periodic time ranges.

An absolute time range indicates the time range from the specified start time to the end time. This time range does not occur cyclically nor has a period, for example, "12:00:00 on January 1, 2000 to 12:00:00 on January 1, 2001".

A periodic time range indicates a periodic time interval, for example, "8:00 on each Monday to 17:00 on each Friday".

For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".

14. Fragmented Packet Matching Mode

The fragmented packet matching mode enables ACL to control fragmented packets more finely.

IP packets may be fragmented during network transmission. When a packet is fragmented, only the first fragment carries L4 information, such as the TCP or UDP port ID, ICMP type, and ICMP code. Other fragmented packets do not carry the L4 information. By default, if an ACL rule carries the fragment flag, only the non-first fragments are matched; if an ACL rule does not carry the fragment flag, all the packets, including the first fragment and all the subsequent fragmented packets, are matched. In addition to the default fragmented packet matching mode, another new fragmented packet matching method is provided. You can switch between the modes on a specified ACL as needed. In the new fragmented packet matching mode, when an ACL rule does not carry the **fragment** option, if a packet is fragmented, the first fragment will be matched with all the user-defined matching fields in the rule (including the L3 and L4 information) and non-first fragments will be matched only with non-L4 information in the rule.

Warning

- In the new fragmented packet matching mode, if an ACL rule does not carry the fragment flag and the matching action is permit, such an ACL rule needs to occupy more hardware entry resources, and, in
-

extreme cases, halves the capacity of hardware policy entries. If such an ACE is configured with **Established** in TCP flag filter control, more hardware policy entry resources will be occupied.

- When you switch the fragmented packet matching mode, the ACL fails for a short period of time.
-

15. Global Control Plane Security ACL

In some application scenarios, an ACL needs to be bound to restrict the source IP host to processing the initial packets in a TCP handshake, instead of conducting restriction after a TCP connection is established. The global control plane security ACL filters packets only through software. It not only reduces the hardware resource consumption but also meets the requirement for processing the initial TCP packets. If you apply a security ACL globally by running a control plane application command, the ACL takes effect on software only.

The global control plane security ACL takes effect on all L2 ports. ACEs are not applied to hardware but only to software, which reduces the hardware resource consumption. During a TCP handshake, the software ACL checks initial TCP packets and filters out the TCP packets that match the ACL.

Note

- The global control plane security ACL is effective to software-based filtering and can be applied only to the inbound direction.
 - The global control plane security ACL is not limited by the configuration of global ACL excluded ports. After the excluded ports are configured, the global control plane security ACL remains effective on the excluded ports.
 - The global control plane security ACL takes effect on both L2 ports and L3 ports. That is, it can take effect on the following types of ports: access port, trunk port, hybrid port, L3 Ethernet port, L2 or L3 aggregation port. It does not take effect on the SVIs or member ports of aggregation ports.
 - The global control plane security ACL can be associated only with the IP standard ACL.
-

1.2 Configuration Task Summary

Select at least one of the following tasks to configure:

- Configuring an IP Standard ACL
- Configuring an IP Extended ACL
- Configuring a MAC Extended ACL
- Configuring an Expert Extended ACL
- Configuring an IPv6 ACL
- Configuring an Expert Advanced ACL (ACL80)

1.3 Configuring an IP Standard ACL

1.3.1 Overview

This section describes how to create and apply an IP standard ACL to control the IPv4 packets entering/leaving a port. You can deny or permit specific IPv4 packets destined to a network so as to control the access of IP users to network resources.

1.3.2 Restrictions and Guidelines

- If a device needs to control users' access to network resources by checking the source IP addresses of packets, you can configure an IP standard ACL.
- The IP standard ACL can be configured on access, convergence, or core devices, depending on user distribution. The IP standard ACL takes effect only on the configured device, and does not affect the other devices in the network.

1.3.3 Configuration Tasks

IP standard ACL configuration includes the following tasks:

- (1) Creating an IP Standard ACL
- (2) Applying an IP Standard ACL
- (3) (Optional) Configuring a Global Security ACL
- (4) (Optional) Configuring a Security Channel
- (5) (Optional) Configuring a Redirect ACL
- (6) (Optional) Configuring the Fragmented Packet Matching Mode
- (7) (Optional) Configuring the SVI Router ACL

1.3.4 Creating an IP Standard ACL

1. Overview

This section describes how to create an IP standard ACL and configure rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all IPv4 packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- Configuring an ACL rule with the **log** option consumes more hardware resources. If all the configured rules have the **log** option, the hardware policy capacity of the device is halved.
- The default output interval of packet matching logs is 0 minutes, that is, no ACL matching log is output. After specifying the **log** option when configuring ACL rules, you also need to configure an output interval; otherwise no matching log is output.
- For a rule with the **log** option, if no packet is matched within the specified time interval, no packet matching log related to the rule is output; if a packet is matched within the specified time interval, the packet matching log related to the rule is output after the time interval expires. The number of matched packets is the total number of packets matching the rule within the time interval, that is, the number of matched packets from the last log output to the current log output.
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured

for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.

- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Create an IP standard ACL and configure rules. Please configure only one task.

- Create a numerically indexed IP standard ACL and configure rules.

```
access-list acl-number { permit | deny } { source-ipv4-address source-ipv4-wildcard | host source-ipv4-address | any } [ time-range time-name ]
```

```
[ log ]
```

- Create a numerically indexed or named IP standard ACL and configure rules. Run the following commands in turn to create an IP standard ACL and configure rules.

```
ip access-list standard { acl-number | acl-name }
```

No IP standard ACL is configured by default.

Run the command to create an IP standard ACL and enter the IP standard ACL configuration mode.

```
[ sn ] { permit | deny } { source-ipv4-address source-ipv4-wildcard | host source-ipv4-address | any } [ time-range time-name ]
```

```
[ log ]
```

There is an ACL rule of deny type in an ACL by default.

(4) (Optional) Configure a remark for the ACL. Please configure only one task.

- Configure a remark for the numerically indexed IP standard ACL.

```
access-list acl-number list-remark comment
```

- Configure remarks for rules in the numerically indexed or named IP standard ACL.

```
list-remark comment
```

No remark is configured for an ACL by default.

(5) (Optional) Configure remarks for rules in the IP standard ACL. Please configure only one task.

- Configure remarks for rules in the numerically indexed IP standard ACL.

```
access-list acl-number remark comment
```

- Configure remarks for rules in the numerically indexed or named IP standard ACL.

```
remark comment
```

No remark is configured for ACL rules by default.

(6) (Optional) Configure an update interval of packet matching logs.

```
ip access-list log-update interval time
```

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

(7) (Optional) Configure a step for rule sequence numbers in the IP standard ACL.

```
ip access-list resequence { acl-number | acl-name } start-sn inc-sn
```

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.3.5 Applying an IP Standard ACL

1. Overview

You can apply an IP standard ACL in global configuration mode or interface configuration mode of a device, or VLAN interface configuration mode to make the IP standard ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an IP standard ACL.
- Configuring the **in** or **out** option indicates that the IP standard ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

```
interface interface-type interface-number
```

- Enter the VLAN interface configuration mode.

```
interface vlan vlan-id
```

(4) Apply the IP standard ACL in interface configuration mode.

```
ip access-group { acl-number | acl-name } { in | out } [ counter-only | control-plane | forward-control-plane | forward-plane ]
```

Running the command enables the IP standard ACL to take effect in specified interface configuration mode, or VLAN interface configuration mode.

1.3.6 Configuring a Global Security ACL

1. Overview

Configuring the global security ACL function can prevent internal access to illegal websites or stop viruses from entering the internal network of an enterprise. In addition, excluded ports of the global security ACL can be configured to permit some special departments in an enterprise to access some external websites.

2. Restrictions and Guidelines

- To implement global protection of the internal network, first configure an ACL.
- You can configure the global security ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured, the global security ACL function is unavailable.
- Disabling the global security ACL function disables configured global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) (Optional) Disable the global security ACL function.

```
global access-group disable
```

The global security ACL function is not disabled by default.

(4) Configure a global security ACL.

```
ip access-group { acl-number | acl-name } global { in | out } [ control-plane | forward-control-plane | forward-plane ]
```

No global security ACL is configured by default.

(5) Enter the interface configuration mode.

```
interface interface-type interface-number
```

(6) (Optional) Configure the global security ACL to take effect on the port.

```
global access-group
```

A port is an excluded port of the global security ACL by default.

(7) (Optional) Configure the global security ACL of the IP type to take effect on the port.

no global ip access-group

A port is an excluded port of the global security ACL of the IP type by default.

1.3.7 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

security global access-group { *acl-number* | *acl-name* }

No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

interface *interface-type interface-number*

security access-group { *acl-number* | *acl-name* }

No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a security channel globally by default.

1.3.8 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

interface *interface-type interface-number*

redirect destination interface *interface-type interface-number acl* { *acl-number* | *acl-name* } **in**

No redirect ACL is configured on a port by default.

After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.3.9 Configuring the Fragmented Packet Matching Mode

1. Overview

This function can be configured to enable ACL to control fragmented packets more finely.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the fragmented packet matching mode.

ip access-list new-fragment-mode { *acl-number* | *acl-name* }

The fragmented packet matching mode of an IP standard ACL or IP extended ACL is the default matching mode by default.

1.3.10 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

svi router-acls enable

1.4 Configuring an IP Extended ACL

1.4.1 Overview

This section describes how to create and apply an IP extended ACL to control the IPv4 packets entering/leaving a port. You can deny or permit specific IPv4 packets destined to a network so as to control the access of IP users to network resources.

1.4.2 Restrictions and Guidelines

- If a device needs to control users' access to network resources by checking the source IP addresses, destination IP addresses, protocol numbers, TCP/UDP source or destination port IDs of packets, you can configure an IP extended ACL.
- The IP extended ACL can be configured on access, convergence, or core devices, depending on user distribution. The IP extended ACL takes effect only on a configured device, but does not affect the other devices in the network.

1.4.3 Configuration Tasks

IP extended ACL configuration includes the following tasks:

(1) Creating an IP Extended ACL

- (2) Applying an IP Extended ACL
- (3) (Optional) Configuring a Global Security ACL
- (4) (Optional) Configuring a Security Channel
- (5) (Optional) Configuring a Redirect ACL
- (6) (Optional) Configuring the Fragmented Packet Matching Mode
- (7) (Optional) Configuring the SVI Router ACL

1.4.4 Creating an IP Extended ACL

1. Overview

This section describes how to create an IP extended ACL and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all IPv4 packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- Configuring an ACL rule with the **log** option consumes more hardware resources. If all the configured rules have the **log** option, the hardware policy capacity of the device is halved.
- The default output interval of packet matching logs is 0 minutes, that is, no ACL matching log is output. After specifying the **log** option when configuring ACL rules, you also need to configure an output interval; otherwise no matching log is output.
- For a rule with the **log** option, if no packet is matched within the specified time interval, no packet matching log related to the rule is output; if a packet is matched within the specified time interval, the packet matching log related to the rule is output after the time interval expires. The number of matched packets is the total number of packets matching the rule within the time interval, that is, the number of matched packets from the last log output to the current log output.
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Configure an IP extended ACL and its rules. Please configure only one task.

- o Configure a numerically indexed IP extended ACL and its rules.

```
access-list acl-number { permit | deny } protocol { source-ipv4-address source-ipv4-wildcard | host
source-ipv4-address | any } { destination-ipv4-address destination-ipv4-wildcard | host destination-ipv4-address |
any } [ [ precedence precedence ] [ tos tos ] ] [ dscp dscp ] ] [ fragment ] [ time-range
time-name ]
```

```
[ log ]
```

- o Configure a numerically indexed or named IP extended ACL and its rules. Run the following commands in turn to configure an IP extended ACL and its rules.

```
ip access-list extended { acl-number | acl-name }
```

No IP extended ACL is configured by default.

Run the command to configure an IP extended ACL and enter the IP extended ACL configuration mode.

```
[ sn ] { permit | deny } protocol { source-ipv4-address source-ipv4-wildcard | host source-ipv4-address
| any } { destination-ipv4-address destination-ipv4-wildcard | host destination-ipv4-address | any } [ [
precedence precedence ] [ tos tos ] ] [ dscp dscp ] ] [ fragment ] [ time-range time-name ]
```

```
[ log ]
```

There is an ACL rule of deny type in an ACL by default.

- (4) (Optional) Configure a remark for the IP extended ACL. Please configure only one task.

- o Configure a remark for a numerically indexed IP extended ACL.

```
access-list acl-number list-remark comment
```

- o Configure a remark for a numerically indexed or named IP extended ACL.

```
list-remark comment
```

No remark is configured for an ACL by default.

- (5) (Optional) Configure remarks for rules in the IP extended ACL. Please configure only one task.

- o Configure remarks for rules in the numerically indexed IP extended ACL.

```
access-list acl-number remark comment
```

- o Configure remarks for rules in the numerically indexed or named ACL.

```
remark comment
```

No remark is configured for ACL rules by default.

- (6) (Optional) Configure an update interval of packet matching logs.

```
ip access-list log-update interval time
```

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

- (7) (Optional) Configure a step for rule sequence numbers in the IP extended ACL.

```
ip access-list resequence { acl-number | acl-name } start-sn inc-sn
```

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.4.5 Applying an IP Extended ACL

1. Overview

This section describes how to apply an IP extended ACL to a device in interface configuration mode, or VLAN interface configuration mode to make the IP extended ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an IP extended ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

```
interface interface-type interface-number
```

- Enter the VLAN interface configuration mode.

```
interface vlan vlan-id
```

(4) Apply an IP extended ACL in interface configuration mode.

```
ip access-group { acl-number | acl-name } { in | out } [ reflect | counter-only | control-plane | forward-control-plane | forward-plane ]
```

Running the command enables an IP extended ACL to take effect in the specified interface configuration mode, or VLAN interface configuration mode.

1.4.6 Configuring a Global Security ACL

1. Overview

Configuring the global security ACL function can prevent internal access to illegal websites or stop viruses from entering the internal network of an enterprise. In addition, excluded ports of the global security ACL can be configured to permit some special departments in an enterprise to access some external websites.

2. Restrictions and Guidelines

- To implement global protection of the internal network, first configure an ACL.
- You can configure the global security ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured, the global security ACL function is unavailable.
- Disabling the global security ACL function disables configured global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) (Optional) Disable the global security ACL function.

```
global access-group disable
```

The global security ACL function is not disabled by default.

(4) Configure a global security ACL.

```
ip access-group { acl-number | acl-name } global { in | out } [ control-plane | forward-control-plane | forward-plane ]
```

No global security ACL is configured by default.

(5) Enter the interface configuration mode.

```
interface interface-type interface-number
```

(6) (Optional) Configure the global security ACL to take effect on the port.

```
global access-group
```

A port is an excluded port of the global security ACL by default.

(7) (Optional) Configure the global security ACL of the IP type to take effect on the port.

```
global ip access-group
```

A port is an excluded port of the global security ACL of the IP type by default.

1.4.7 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

security global access-group { *acl-number* | *acl-name* }

No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

interface *interface-type interface-number*

security access-group { *acl-number* | *acl-name* }

No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a global security channel by default.

1.4.8 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

```
interface interface-type interface-number
```

```
redirect destination interface interface-type interface-number acl { acl-number | acl-name } in
```

No redirect ACL is configured on a port by default.

After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.4.9 Configuring the Fragmented Packet Matching Mode

1. Overview

This function can be configured to enable ACL to control fragmented packets more finely.

2. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Configure the fragmented packet matching mode.

```
ip access-list new-fragment-mode { acl-number | acl-name }
```

The fragmented packet matching mode of an IP standard ACL or IP extended ACL is the default matching mode by default.

1.4.10 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Configure the SVI router ACL.

```
svi router-acls enable
```

1.5 Configuring a MAC Extended ACL

1.5.1 Overview

This section describes how to create and apply a MAC extended ACL to control the L2 packets entering/leaving a port. You can deny or permit specific L2 packets destined to a network so as to control the access of users to network resources based on the L2 packet headers.

1.5.2 Restrictions and Guidelines

- If a device needs to control users' access to network resources based on the L2 packet information (such as the MAC addresses of users' PCs), you can configure a MAC extended ACL.
- The MAC extended ACL can be configured on access, convergence, or core devices, depending on user distribution. The MAC extended ACL takes effect only on the configured device, but does not affect other devices in the network.

1.5.3 Configuration Tasks

MAC extended ACL configuration includes the following tasks:

(1) Creating a MAC Extended ACL

- (2) Applying a MAC Extended ACL
- (3) (Optional) Configuring a Security Channel
- (4) (Optional) Configuring a Redirect ACL
- (5) (Optional) Configuring the SVI Router ACL

1.5.4 Creating a MAC Extended ACL

1. Overview

This section describes how to create a MAC extended ACL and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all Ethernet L2 packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

- (1) Enter the privileged EXEC mode.

```
enable
```

- (2) Enter the global configuration mode.

```
configure terminal
```

- (3) Configure a MAC extended ACL and its rules. Please configure only one task.

- o Configure a numerically indexed MAC extended ACL and its rules.

```
access-list acl-number { permit | deny } { source-mac-address source-mac-wildcard | host source-mac-address | any } { destination-mac-address destination-mac-wildcard | host destination-mac-address | any } [ ethernet-type ] [ cos cos-value [ inner cos-value ] ] [ time-range time-name ]
```

- o Configure a numerically indexed or named MAC extended ACL and its rules. Run the following commands in turn to configure a MAC extended ACL and its rules.

```
mac access-list extended { acl-number | acl-name }
```

No MAC extended ACL is configured by default.

Run the command to configure a MAC extended ACL and enter the MAC extended ACL configuration mode.

```
[sn] { permit | deny } { source-mac-address source-mac-wildcard | host source-mac-address | any } {
destination-mac-address destination-mac-wildcard | host destination-mac-address | any } [ ethernet-
type ] [ cos cos-value [ inner cos-value ] ] [ time-range time-name ]
```

There is an ACL rule of deny type in an ACL by default.

(4) (Optional) Configure a remark for the ACL. Please configure only one task.

- o Configure a remark for the numerically indexed ACL.

```
access-list acl-number list-remark comment
```

- o Configure remarks for rules in the numerically indexed or named ACL.

```
list-remark comment
```

No remark is configured for an ACL by default.

(5) (Optional) Configure remarks for ACL rules. Please configure only one task.

- o Configure remarks for rules in the numerically indexed ACL.

```
access-list acl-number remark comment
```

- o Configure remarks for rules in the numerically indexed or named ACL.

```
remark comment
```

No remark is configured for ACL rules by default.

(6) (Optional) Configure a step for rule sequence numbers in the ACL.

```
mac access-list resequence { acl-number | acl-name } start-sn inc-sn
```

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.5.5 Applying a MAC Extended ACL

1. Overview

This section describes how to apply a MAC extended ACL to a device in interface configuration mode, or VLAN interface configuration mode to make the MAC extended ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply a MAC extended ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.

- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

interface vlan *vlan-id*

(4) Apply a MAC extended ACL in interface configuration mode.

mac access-group { *acl-number* | *acl-name* } { **in** | **out** } [**counter-only** | **control-plane** | **forward-control-plane** | **forward-plane**]

Running the command enables a MAC extended ACL to take effect in the specified interface configuration mode, or VLAN interface configuration mode.

1.5.6 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- o Configure a global security channel.

security global access-group { *acl-number* | *acl-name* }

No global security channel is configured by default.

- o Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

interface *interface-type interface-number*

security access-group { *acl-number* | *acl-name* }

No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a security channel globally by default.

1.5.7 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

```
interface interface-type interface-number
```

```
redirect destination interface interface-type interface-number acl { acl-number | acl-name } in
```

No redirect ACL is configured on a port by default.

After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.5.8 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Configure the SVI router ACL.

```
svi router-acls enable
```

1.6 Configuring an Expert Extended ACL

1.6.1 Overview

This section describes how to create and apply an expert extended ACL to control the packets entering/leaving the port. You can deny or permit specific packets destined to a network.

1.6.2 Restrictions and Guidelines

- If a device needs to control users' access to network resources by using IP ACL rules, MAC extended ACL rules, and VLANs in a mixed manner, you can configure an expert extended ACL.
- You can perform this configuration on an access, convergence, or core device based on the distribution of users. The configuration takes effect only on a configured device, but does not affect other devices in the network.

1.6.3 Configuration Tasks

Expert extended ACL configuration includes the following tasks:

- (1) Creating an Expert Extended ACL
- (2) Applying an Expert Extended ACL
- (3) (Optional) Configuring a Global Security ACL
- (4) (Optional) Configuring a Security Channel
- (5) (Optional) Configuring a Redirect ACL
- (6) (Optional) Configuring the Fragmented Packet Matching Mode
- (7) (Optional) Configuring the SVI Router ACL

1.6.4 Creating an Expert Extended ACL

1. Overview

This section describes how to create an expert extended ACL and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

- (1) Enter the privileged EXEC mode.

enable

- (2) Enter the global configuration mode.

configure terminal

- (3) Configure an expert extended ACL and its rules. Please configure only one task.

- Configure a numerically indexed expert extended ACL and its rules.

```
access-list acl-number { permit | deny } [ protocol | [ ethernet-type ] [ cos [ cos-value ] [ inner cos-value ] ] ] [ [ VID [ vlan-id ] [ inner vlan-id ] ] ] { source-ipv4-address source-ipv4-wildcard | host source-ipv4-address | any } { source-mac-address source-mac-wildcard | host source-mac-address | any } { destination-ipv4-address destination-ipv4-wildcard | host destination-ipv4-address | any } { destination-mac-address destination-mac-wildcard | host destination-mac-address | any } [ [ precedence precedence ] [ tos tos ] ] [ dscp dscp ] ] [ fragment ] [ time-range time-name ]
```

- o Configure a numerically indexed or named expert extended ACL and its rules. Run the following commands in turn to configure an expert extended ACL and its rules.

expert access-list extended { *acl-number* | *acl-name* }

No expert extended ACL is configured by default.

Run the command to configure an expert extended ACL and enter the expert extended ACL configuration mode.

```
[ sn ] { permit | deny } [ protocol | [ ethernet-type ] [ cos [ cos-value ] [ inner cos-value ] ] ] [ VID [ vlan-id ] [ inner vlan-id ] ] { source-ipv4-address source-ipv4-wildcard | host source-ipv4-address | any } { source-mac-address source-mac-wildcard | host source-mac-address | any } { destination-ipv4-address destination-ipv4-wildcard | host destination-ipv4-address | any } { destination-mac-address destination-mac-wildcard | host destination-mac-address | any } [ [ precedence precedence ] [ tos tos ] ] [ [ dscp dscp ] [ fragment ] [ time-range time-name ]
```

There is an ACL rule of deny type in an ACL by default.

- (4) (Optional) Configure a remark for the ACL. Please configure only one task.

- o Configure a remark for the numerically indexed ACL.

access-list *acl-number* **list-remark** *comment*

- o Configure remarks for rules in the numerically indexed or named ACL.

list-remark *comment*

No remark is configured for an ACL by default.

- (5) (Optional) Configure remarks for ACL rules. Please configure only one task.

- o Configure remarks for rules in the numerically indexed ACL.

access-list *acl-number* **remark** *comment*

- o Configure remarks for rules in the numerically indexed or named ACL.

remark *comment*

No remark is configured for ACL rules by default.

- (6) (Optional) Configure a step for rule sequence numbers in the ACL.

expert access-list resequence { *acl-number* | *acl-name* } *start-sn* *inc-sn*

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.6.5 Applying an Expert Extended ACL

1. Overview

You can apply an expert extended ACL to a device in global configuration mode or interface configuration mode, or VLAN interface configuration mode to make the expert extended ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an expert extended ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or

those forwarded by the device.

- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

interface vlan *vlan-id*

(4) Apply an expert extended ACL in interface configuration mode.

expert access-group { *acl-number* | *acl-name* } { **in** | **out** } [**counter-only** | **control-plane** | **forward-control-plane** | **forward-plane**]

Run the command to enable an expert extended ACL to take effect on a specified port.

1.6.6 Configuring a Global Security ACL

1. Overview

Configuring the global security ACL function can prevent internal access to illegal websites or stop viruses from entering the internal network of an enterprise. In addition, excluded ports of the global security ACL can be configured to permit some special departments in an enterprise to access some external websites.

2. Restrictions and Guidelines

- To implement global protection of the internal network, first configure an ACL.
- You can configure the global security ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.

- An ACL can contain no rules. When no rule is configured, the global security ACL function is unavailable.
- Disabling the global security ACL function disables configured global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) (Optional) Disable the global security ACL function.

```
global access-group disable
```

The global security ACL function is not disabled by default.

(4) Configure a global security ACL.

```
expert access-group { acl-number | acl-name } global { in | out } [ control-plan | forward-control-plane | forward-plane ]
```

No global security ACL is configured by default.

(5) Enter the interface configuration mode.

```
interface interface-type interface-number
```

(6) (Optional) Configure the global security ACL to take effect on the port.

```
global access-group
```

A port is an excluded port of the global security ACL by default.

1.6.7 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.

- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

security global access-group { *acl-number* | *acl-name* }

No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

interface *interface-type interface-number*

security access-group { *acl-number* | *acl-name* }

No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a security channel globally by default.

1.6.8 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- o Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

```
interface interface-type interface-number
```

```
redirect destination interface interface-type interface-number acl { acl-number | acl-name } in
```

No redirect ACL is configured on a port by default.

After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.6.9 Configuring the Fragmented Packet Matching Mode

1. Overview

This function can be configured to enable ACL to control fragmented packets more finely.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the fragmented packet matching mode.

```
expert access-list new-fragment-mode { acl-number | acl-name }
```

1.6.10 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

```
svi router-acls enable
```

1.7 Configuring an IPv6 ACL

1.7.1 Overview

This section describes how to create and apply an IPv6 ACL to control the IPv6 packets entering/leaving the port. You can deny or permit specific IPv6 packets destined to a network so as to control the access of IPv6 users to network resources.

1.7.2 Restrictions and Guidelines

- To control IPv6 users' access to network resources, configure an IPv6 ACL.
- You can perform this configuration on an access, convergence, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.

1.7.3 Configuration Tasks

IPv6 ACL configuration includes the following tasks:

- (1) Creating an IPv6 ACL
- (2) Applying an IPv6 ACL
- (3) (Optional) Configuring a Global Security ACL
- (4) (Optional) Configuring a Security Channel
- (5) (Optional) Configuring a Redirect ACL
- (6) (Optional) Configuring the SVI Router ACL

1.7.4 Creating an IPv6 ACL

1. Overview

This section describes how to create an IPv6 ACL and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all IPv6 packets from entering the device.
- To make some ACL rules take effect at specified time or expire at specified time, for example, make an ACL effective within some time ranges in a week, configure an ACL rule with the **time-range** option.
- When configuring an ACL rule with the **time-range** option, configure the time range option. For the configuration of time ranges, see "Time Range" in the "Basic Configuration Guide".
- Configuring an ACL rule with the **log** option consumes more hardware resources. If all the configured rules have the **log** option, the hardware policy capacity of the device is halved.
- The default output interval of packet matching logs is 0 minutes, that is, no ACL matching log is output. After specifying the **log** option when configuring ACL rules, you also need to configure an output interval; otherwise no matching log is output.
- For a rule with the **log** option, if no packet is matched within the specified time interval, no packet matching

log related to the rule is output; if a packet is matched within the specified time interval, the packet matching log related to the rule is output after the time interval expires. The number of matched packets is the total number of packets matching the rule within the time interval, that is, the number of matched packets from the last log output to the current log output.

- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an IPv6 ACL and enter the IPv6 ACL configuration mode.

ipv6 access-list *acl-name*

No IPv6 ACL is configured by default.

(4) Configure IPv6 ACL rules. Please configure only one task.

- Configure IPv6 ACL rules of TCP or UDP.


```
[ sn ] { permit | deny } [ protocol { source-ipv6-prefix / prefix-length | source-ipv6-address source-ipv6-mask | host source-ipv6-address | any } { { destination-ipv6-prefix / prefix-length | destination-ipv6-address destination-ipv6-mask | host destination-ipv6-address | any } [ op dstport ] [ cos value [ inner value ] ] [ { any | host source-mac-address | source-mac-address source-mac-wildcard } { any | host destination-mac-address | destination-mac-address destination-mac-wildcard } ] [ dscp dscp ] [ flow-label flow-label ] [ fragment ] [ vid vlan-id ] [ time-range time-name ] [ log ]
```
- Configure IPv6 ACL rules of protocols other than TCP or UDP.


```
[ sn ] { permit | deny } [ protocol { source-ipv6-prefix / prefix-length | source-ipv6-address source-ipv6-mask | host source-ipv6-address | any } { destination-ipv6-prefix / prefix-length | destination-ipv6-address destination-ipv6-mask | host destination-ipv6-address | any } ] [ { any | host source-mac-address | source-mac-address source-mac-wildcard } { any | host destination-mac-address | destination-mac-address destination-mac-wildcard } ] [ dscp dscp ] [ flow-label flow-label ] [ fragment ] [ vid vlan-id ] [ time-range time-name ] [ log ]
```

(5) (Optional) Configure a remark for the ACL.

list-remark *comment*

No remark is configured for an ACL by default.

(6) (Optional) Configure remarks for ACL rules.

remark *comment*

No remark is configured for ACL rules by default.

(7) (Optional) Configure an update interval of packet matching logs.

ipv6 access-list log-update interval *time*

The default update interval of packet matching logs is 0 minutes, that is, no ACL matching log is output.

(8) (Optional) Configure a step for rule sequence numbers in the ACL.

ipv6 access-list resequence *acl-name start-sn inc-sn*

Both the start value and step of ACL rule sequence numbers are **10** by default.

1.7.5 Applying an IPv6 ACL

1. Overview

This section describes how to apply an IPv6 ACL to a device in interface configuration mode, or VLAN interface configuration mode to make the IPv6 ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an IPv6 ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.
- Configuring the **reflect** option enables the reflexive ACL.
- Configure the **counter-only** option to count the packets with some characteristics. The counting function takes effect only for permit rules but not for deny rules in an ACL.
- After an ACL is used as a **counter-only** ACL, the counting function cannot be globally enabled for the ACL, and the ACL cannot be applied globally or on ports as a common ACL. That is, ACLs with the same *acl-number* or *acl-name* cannot be used as a **counter-only** ACL and a common ACL at the same time.
- If the **control-plane** option is configured, the ACL is effective for software only so as to save hardware resources.
- If the **forward-plane** option is configured, the ACL is effective for hardware only.
- If the **forward-control-plane** option is configured, the ACL is effective for both software and hardware.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

interface *interface-type interface-number*

- Enter the VLAN interface configuration mode.

interface vlan *vlan-id*

(4) Apply an IPv6 ACL in interface configuration mode.

```
ipv6 traffic-filter acl-name { in | out } [ counter-only | control-plane | forward-control-plane | forward-plane ]
```

Run the command to enable an IPv6 ACL to take effect in global configuration mode or specified interface configuration mode, or VLAN interface configuration mode.

1.7.6 Configuring a Global Security ACL

1. Overview

Configuring the global security ACL function can prevent internal access to illegal websites or stop viruses from entering the internal network of an enterprise. In addition, excluded ports of the global security ACL can be configured to permit some special departments in an enterprise to access some external websites.

2. Restrictions and Guidelines

- To implement global protection of the internal network, first configure an ACL.
- You can configure the global security ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured, the global security ACL function is unavailable.
- Disabling the global security ACL function disables configured global security ACLs.
- Configuring a port as an excluded port disables the global security ACL on the port.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) (Optional) Disable the global security ACL function.

```
global access-group disable
```

The global security ACL function is not disabled by default.

(4) Enter the interface configuration mode.

```
interface interface-type interface-number
```

(5) (Optional) Configure the global security ACL to take effect on the port.

```
global access-group
```

A port is an excluded port of the global security ACL by default.

1.7.7 Configuring a Security Channel

1. Overview

The security channel function enables the packets conforming to the security channel rules to bypass the access control related services. For example, IEEE 802.1x access control is enabled on a port of the uplink

device connected to a user host, and a security channel can be configured to permit the user to log in to a site to download the authentication client before 802.1x authentication.

2. Restrictions and Guidelines

- To implement the security channel function, first configure an ACL.
- You can configure the security channel function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- An ACL can contain no rules. When no rule is configured in an ACL, the security channel function is unavailable.
- To make a security channel take effect on a port, configure the security channel on the specified port only; to make a security channel globally, configure a security channel in global configuration mode.
- If you have configured a global security channel but want to disable the security channel on some ports, configure these ports as excluded ports of the global security channel.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a specified ACL as a security channel. Please configure only one task.

- Configure a global security channel.

security global access-group *acl-name*

No global security channel is configured by default.

- Configure a security channel on a port. Run the following commands in turn to configure a security channel on a port.

interface *interface-type interface-number*

security access-group *acl-name*

No security channel is configured on a port by default.

(4) (Optional) Configure a port as an excluded port of the security channel.

security uplink enable

No port is configured as an excluded port of a security channel globally by default.

1.7.8 Configuring a Redirect ACL

1. Overview

This section describes how to configure the redirect ACL function on a specified port or globally, to redirect the matched packets entering the port or all the ports to a specified port for forwarding.

2. Restrictions and Guidelines

- To implement the redirect ACL function, configure an ACL first.
- You can configure the redirect ACL function on an access, aggregation, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.
- The redirect ACL function can be configured on an Ethernet port, aggregation port, or SVI only.
- The packet to be redirected must be an L2 forwarded packet (that is, if a packet is forwarded from VLAN 2 to VLAN 3, it cannot be redirected), and the destination port of redirection must be in the same VLAN as the source port.
- An ACL can contain no rules. If no rule is configured in an ACL, the redirect ACL function is unavailable.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a redirect ACL. Please configure only one task.

- Configure a redirect ACL on a port. Run the following commands in turn to configure a redirect ACL on a port.

interface *interface-type interface-number*

redirect destination interface *interface-type interface-number* **acl** *acl-name* **in**

No redirect ACL is configured on a port by default.

After the command is executed, the incoming packets of a specified port that match the ACL rules are redirected to a destination port for forwarding.

1.7.9 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

```
svi router-acls enable
```

1.8 Configuring an Expert Advanced ACL (ACL80)

1.8.1 Overview

When the fixed matching fields of the IP standard ACL, IP extended ACL, MAC extended ACL, expert extended ACL, and IPv6 ACL all fail to meet requirements, you can configure an ACL80 to define the packet fields to be matched.

1.8.2 Restrictions and Guidelines

- To implement the ACL80 function, first configure an expert advanced ACL.
- You can perform this configuration on an access, convergence, or core device based on the distribution of users. The configuration takes effect only on the local device, but does not affect other devices in the network.

1.8.3 Configuration Tasks

The ACL80 configuration includes the following tasks:

- (1) Creating an ACL80
- (2) Applying an ACL80
- (3) (Optional) Configuring the SVI Router ACL

1.8.4 Creating an ACL80

1. Overview

This section describes how to create an ACL80 and configure its rules.

2. Restrictions and Guidelines

- An ACL can contain no rules. By default, when no rules are configured in an ACL, one rule statement of denying all data flows is hidden in the ACL to prohibit all packets from entering the device.
- During the actual network maintenance, if many ACLs or rules are configured, but no remark is configured for these ACLs or rules, it is difficult to distinguish the purposes of these ACLs or rules. Configuring remarks for ACLs or rules can help you understand the purpose of the ACLs.
- Before configuring a step for ACL rule sequence numbers, you must first configure an ACL.

3. Procedure

- (1) Enter the privileged EXEC mode.

```
enable
```

- (2) Enter the global configuration mode.

```
configure terminal
```

- (3) Configure an expert advanced ACL and enter the expert advanced ACL configuration mode.

```
expert access-list advanced acl-name
```

No expert advanced ACL is configured by default.

(4) (Optional) Configure rules in the expert advanced ACL.

```
[ sn ] { permit | deny } hex hex-mask offset
```

Run the command to configure user-defined rules for an ACL in expert advanced ACL mode.

(5) (Optional) Configure a remark for the ACL.

```
list-remark comment
```

No remark is configured for an ACL by default.

(6) (Optional) Configure remarks for ACL rules.

```
remark comment
```

No remark is configured for ACL rules by default.

1.8.5 Applying an ACL80

1. Overview

This section describes how to apply an expert advanced ACL to a device in interface configuration mode, or VLAN interface configuration mode to make the expert advanced ACL take effect.

2. Restrictions and Guidelines

- Based on the user distribution, on the access, convergence, or core devices, in specified interface configuration mode, or VLAN interface configuration mode, you can apply an expert advanced ACL.
- Configuring the **in** or **out** option indicates that the ACL takes effect for the packets entering the device or those forwarded by the device.

3. Procedure

(1) Enter the privileged EXEC mode.

```
enable
```

(2) Enter the global configuration mode.

```
configure terminal
```

(3) Enter the interface configuration mode.

- Enter the interface configuration mode.

```
interface interface-type interface-number
```

- Enter the VLAN interface configuration mode.

```
interface vlan vlan-id
```

(4) Apply an expert advanced ACL in interface configuration mode.

```
expert access-group { acl-number | acl-name } { in | out }
```

1.8.6 Configuring the SVI Router ACL

1. Overview

The SVI router ACL function can be configured to enable the ACL applied to an SVI to take effect only for the inter-VLAN routed packets.

2. Restrictions and Guidelines

To implement this function, first configure an ACL.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the SVI router ACL.

svi router-acls enable

1.9 Monitoring


Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

 Caution

Running the **clear** commands may interrupt services due to loss of important information.

Run the **debug** command to output debugging information.

 Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Table 1-1ACL Monitoring

Command	Purpose
show access-lists [<i>acl-number</i> <i>acl-name</i>] [summary]	Displays a basic ACL.
show redirect [interface <i>interface-type interface-number</i>]	Displays the redirection entries bound to a specified port. If no port is specified, the redirection entries bound to all the ports are displayed.
show access-group [interface <i>interface-type interface-number</i> vlan <i>vlan-id</i>]	Displays the configuration of an ACL applied to a port.

Command	Purpose
show ip access-group [interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i>]	Displays the configuration of an IP standard ACL and an extended ACL applied to a port.
show mac access-group [interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i>]	Displays the configuration of a MAC extended ACL applied to a port.
show expert access-group [interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i>]	Displays the configuration of an expert extended ACL applied to a port.
show ipv6 traffic-filter [interface <i>interface-type</i> <i>interface-number</i> vlan <i>vlan-id</i>]	Displays the configuration of an IPv6 ACL applied to a port.
show acl res [dev <i>dev-num</i> [slot <i>slot-num</i>]]	Displays information about all ternary content-addressable memory (TCAMs) or a specified TCAM.
show svi router-acls state	Checks whether an ACL applied to an SVI takes effect on L2 and L packets.
show qos res [dev <i>dev-num</i> [slot <i>slot-num</i>]]	Displays information about all the QoS resources or a specified QoS resource.
show acl res detail [dev <i>dev-num</i> [slot <i>slot-num</i>]]	Displays usage details about all TCAMs or a specified TCAM.
clear counters access-list [<i>acl-number</i> <i>acl-name</i>]	Clears the number of packets matching an ACL.
clear access-list counters [<i>acl-number</i> <i>acl-name</i>]	Clears the number of packets matching ACL deny rules.
debug acl acl event	Debugs the ACL running process.
debug acl acl client-show	Displays ACL client information.
debug acl acl acl-show	Displays ACLs created on all ACL clients.

1.10 Examples

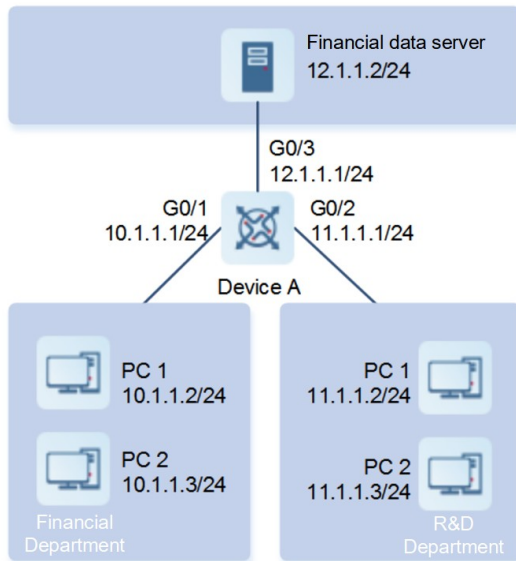
1.10.1 Configuring an IP Standard ACL

1. Requirements

An IP standard ACL needs to be configured to prevent the departments other than the financial department from accessing the financial data server.

2. Topology

Figure 1-1 Topology of IP Standard ACL Application Scenario



3. Notes

- Configure an IP standard ACL on device A and add access rules.
- Apply the IP standard ACL to the outbound direction of the port connected to the financial data server on device A.

4. Procedure

(1) Configure an IP standard ACL and add access rules.

On device A, configure an IP standard ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip access-list standard 1
DeviceA(config-std-nacl)# permit 10.1.1.0 0.0.0.255
DeviceA(config-std-nacl)# deny 11.1.1.1 0.0.0.255
DeviceA(config-std-nacl)# exit
```

(2) Apply the IP standard ACL to a port.

On device A, apply the IP standard ACL to the outbound direction of the port connected to the financial data server.

```
DeviceA(config)# interface gigabitethernet 0/3
DeviceA(config-if-GigabitEthernet 0/3)# ip access-group 1 out
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA# show access-lists
```

```
ip access-list standard 1
10 permit 10.1.1.0 0.0.0.255
20 deny 11.1.1.0 0.0.0.255

DeviceA# show access-group
ip access-group 1 out
Applied On interface GigabitEthernet 0/3
```

Ping the financial data server from a PC of the R&D department and confirm that the ping operation fails.

Ping the financial data server from a PC of the financial department and confirm that the ping operation succeeds.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ip access-list standard 1
 10 permit 10.1.1.0 0.0.0.255
 20 deny 11.1.1.0 0.0.0.255
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip access-group 1 out
 ip address 12.1.1.1 255.255.255.0
!
```

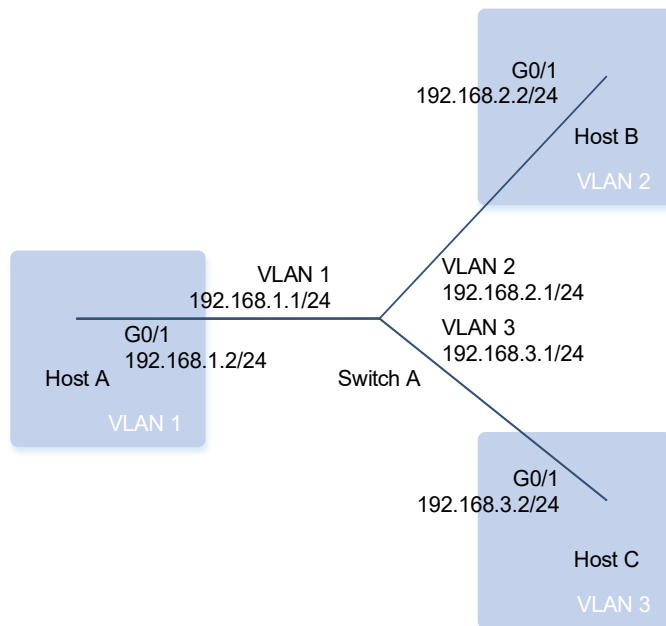
1.10.2 Configuring an IP Extended ACL

1. Requirements

Host A (VLAN 1), host B (VLAN 2), and host C (VLAN 3) are directly connected to the device which functions as the gateway of all the hosts. Requirement 1: The ping operation fails between VLAN 2 and VLAN 3, but succeeds between VLAN 1 and VLAN 2, and between VLAN 1 and VLAN 3. Requirement 2: The DHCP packets of VLAN 1 and VLAN 2 are unreachable to each other, but the communication using other protocols is normal. Requirement 3: The host in VLAN 1 cannot to access VLAN 3 through telnet or SSH, but the communication using other protocols is normal.

2. Topology

Figure 1-1 Topology of IP Extended ACL Application Scenario



3. Notes

- On switch A, configure an IP extended ACL and add an access rule of filtering out packets received by UDP port 67 or 68 to meet requirement 2. On host C, configure an IP extended ACL and add an access rule of filtering out packets received by ACL ports 23 and 22 to meet requirement 3.
- On switch A, apply the IP extended ACL to VLAN 1 interface, VLAN 2 interface, and VLAN 3 interface. On host C, apply the IP extended ACL to the line connected to the device.

4. Procedure

- (1) Configure IP addresses for all the device ports (omitted).
- (2) Configure an IP extended ACL and add access rules.

On switch A, configure an IP extended ACL and add access rules.

```
SwitchA> enable
SwitchA# configure terminal
SwitchA(config)# ip access-list extended inter_vlan_access1
SwitchA(config-ext-nacl)# deny udp any eq bootps any eq bootpc
SwitchA(config-ext-nacl)# deny udp any eq bootpc any eq bootps
SwitchA(config-ext-nacl)# remark //Deny DHCP packets.
SwitchA(config-ext-nacl)# permit ip any any
SwitchA(config-ext-nacl)# remark //Permit the communication using other
packets.
SwitchA(config-ext-nacl)# exit
SwitchA(config)# ip access-list extended inter_vlan_access2
```



```

SwitchA(config-ext-nacl)# deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
SwitchA(config-ext-nacl)# remark //Deny the mutual access between VLAN 2 and
VLAN 3.
SwitchA(config-ext-nacl)# deny udp any eq bootpc any eq bootps
SwitchA(config-ext-nacl)# deny udp any eq bootps any eq bootpc
SwitchA(config-ext-nacl)# remark //Deny DHCP packets.
SwitchA(config-ext-nacl)# permit ip any any
SwitchA(config-ext-nacl)# remark //Permit the communication using other
packets.
SwitchA(config-ext-nacl)# exit
SwitchA(config)# ip access-list extended inter_vlan_access3
SwitchA(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
SwitchA(config-ext-nacl)# remark //Deny the mutual access between VLAN 2 and
VLAN 3.
SwitchA(config-ext-nacl)# permit ip any any
SwitchA(config-ext-nacl)# remark //Permit the communication using other
packets.
SwitchA(config-ext-nacl)# exit

```

On host C, configure an IP extended ACL and add access rules.

```

HostC> enable
HostC# configure terminal
HostC(config)# ip access-list extended access_deny
HostC(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 eq telnet any eq telnet
HostC(config-ext-nacl)# remark //Deny VLAN 1 access to VLAN 3 through telnet.
HostC(config-ext-nacl)# deny tcp 192.168.1.0 0.0.0.255 eq 22 any eq 22
HostC(config-ext-nacl)# remark //Deny VLAN 1 access to VLAN 3 through SSH.
HostC(config-ext-nacl)# exit

```

(3) Apply the IP extended ACLs.

On switch A, apply the IP extended ACL to the corresponding ports.

```

SwitchA(config)# interface vlan 1
SwitchA(config-if-VLAN 1)# ip access-group inter_vlan_access1 in
SwitchA(config-if-VLAN 1)# exit
SwitchA(config)# interface vlan 2
SwitchA(config-if-VLAN 2)# ip access-group inter_vlan_access2 in
SwitchA(config-if-VLAN 2)# exit
SwitchA(config)# interface vlan 3
SwitchA(config-if-VLAN 3)# ip access-group inter_vlan_access3 in
SwitchA(config-if-VLAN 3)# exit

```

On host C, apply the IP extended ACL to the line connected to the device.

```

hostC(config)# line vty 0
hostC(config-line)# access-class access_deny in
hostC(config-line)# exit

```

5. Verification

- (1) Verify the connectivity.

The ping operation succeeds between VLAN 1 and VLAN 2, and between VLAN 1 and VLAN 3.

```
hostA# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
 < press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms
hostA#
hostA# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
 < press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms
```

The ping operation fails between VLAN 2 and VLAN 3.

```
hostB# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
 < press Ctrl+C to break >
.....
Success rate is 0 percent (0/5)
```

- (2) The host in VLAN 1 cannot access VLAN 3 through telnet.

```
hostA# ping 192.168.3.2
Sending 5, 100-byte ICMP Echoes to 192.168.3.2, timeout is 2 seconds:
 < press Ctrl+C to break >
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/10 ms
hostA#
hostA# telnet 192.168.3.2
Trying 192.168.3.2, 23...
% Destination unreachable; gateway or host down
```

6. Configuration Files

- Switch A configuration file

```
hostname SwitchA
!
vlan 1
!
vlan 2
!
vlan 3
!
ip access-list extended inter_vlan_access1
```

```
10 deny udp any eq bootps any eq bootpc
20 deny udp any eq bootpc any eq bootps
remark //Deny DHCP packets.
30 permit ip any any
remark //Permit the communication using other packets.
!
ip access-list extended inter_vlan_access2
10 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
remark //Deny the mutual access between VLAN 2 and VLAN 3.
20 deny udp any eq bootpc any eq bootps
30 deny udp any eq bootps any eq bootpc
remark //Deny DHCP packets.
40 permit ip any any
remark //Permit the communication using other packets.
!
ip access-list extended inter_vlan_access3
10 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
remark //Deny the mutual access between VLAN 2 and VLAN 3.
20 permit ip any any
remark //Permit the communication using other packets.
!
interface GigabitEthernet 1/0
 switchport access vlan 1
 description link_to_hostA
!
interface GigabitEthernet 1/1
 switchport access vlan 2
 description link_to_hostB
!
interface GigabitEthernet 1/2
 switchport access vlan 3
 description link_to_hostC
!
interface VLAN 1
 ip access-group inter_vlan_access1 in
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 2
 ip access-group inter_vlan_access2 in
 ip address 192.168.2.1 255.255.255.0
!
interface VLAN 3
 ip access-group inter_vlan_access3 in
 ip address 192.168.3.1 255.255.255.0
!
```

- Host A configuration file

```
hostname HostA
!
interface GigabitEthernet 0/1
 ip address 192.168.1.2 255.255.255.0
!
```

- Host B configuration file

```
hostname HostB
!
interface GigabitEthernet 0/1
 ip address 192.168.2.2 255.255.255.0
!
```

- Host C configuration file

```
hostname HostC
!
ip access-list extended access_deny
 10 deny tcp 192.168.1.0 0.0.0.255 eq telnet any eq telnet
  remark //Denies VLAN 1 access to VLAN 3 through telnet.
 20 deny tcp 192.168.1.0 0.0.0.255 eq 22 any eq 22
  remark //Deny VLAN 1 access to VLAN 3 through SSH.
!
interface GigabitEthernet 0/1
 ip address 192.168.3.2 255.255.255.0
!
line vty 0
 access-class access_deny in
 login
 password orion_B26Q
!
```

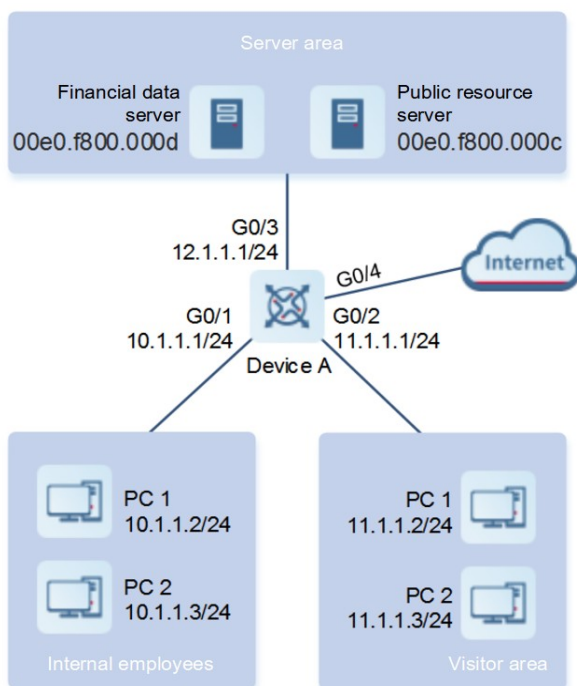
1.10.3 Configuring a MAC Extended ACL

1. Requirements

A MAC extended ACL needs to be configured to restrict the resources accessible to visitors.

2. Topology

Figure 1-1 Topology of MAC Extended ACL Application Scenario



3. Notes

- On device A, configure a MAC extended ACL and add access rules. The PCs in the visitor area are allowed to access the Internet and the company's internal public server, but are not allowed to access the company's financial data server, that is, the PCs are prohibited from accessing the server with MAC address 00e0.f800.000d.
- On device A, apply the MAC extended ACL to the inbound direction of a port connected to the visitor area.

4. Procedure

(1) Configure a MAC extended ACL and add access rules.

On device A, configure a MAC extended ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# mac access-list extended 700
DeviceA(config-mac-nacl)# deny any host 00e0.f800.000d
DeviceA(config-mac-nacl)# permit any any
DeviceA(config-mac-nacl)# exit
```

(2) Apply the MAC extended ACL to a port.

On device A, apply the ACL to the inbound direction of the port connected to the visitor area.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# mac access-group 700 in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA# show access-lists
mac access-list extended 700
10 deny any host 00e0.f800.000d etype-any
20 permit any any etype-any
DeviceA# show access-group
mac access-group 700 in
Applied On interface GigabitEthernet 0/2
```

Ping the financial data server from a visitor PC and confirm that the ping operation fails.

Ping the public resource server from a visitor PC and confirm that the ping operation succeeds.

Access the Internet through a visitor PC, for example, access www.baidu.com, and confirm that the home page can be opened.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
mac access-list extended 700
 10 deny any host 00e0.f800.000d
 20 permit any any
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 mac access-group 700 in
 ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip address 12.1.1.1 255.255.255.0
!
```

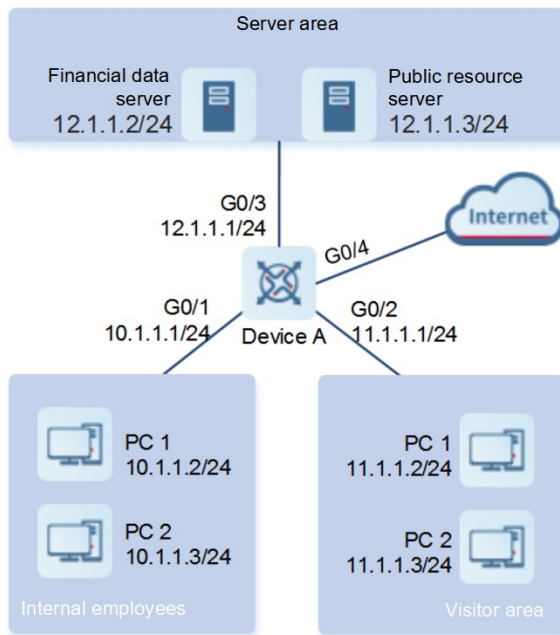
1.10.4 Configuring an Expert Extended ACL

1. Requirements

An expert extended ACL needs to be configured to restrict the resources accessible to visitors. Visitors cannot access the PCs of internal employees or the financial data server of the company, but can access the public resource server.

2. Topology

Figure 1-1 Topology of Expert Extended ACL Application Scenario



3. Notes

- On device A, configure an expert extended ACL and add access rules, including:
 - Prohibiting the hosts in the visitor area from sending packets destined to the network segment of internal employees' PCs.
 - Prohibiting visitors from accessing the financial data server.
 - Permitting all the other packets to pass through.
- On device A, apply the ACL to the inbound direction of the port connected to the visitor area.

4. Procedure

(1) Configure an expert extended ACL and add access rules.

On device A, configure an expert extended ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# expert access-list extended 2700
DeviceA(config-exp-nacl)# deny ip any any 10.1.1.0 0.0.0.255 any
DeviceA(config-exp-nacl)# deny ip any any host 12.1.1.2 any
DeviceA(config-exp-nacl)# permit any any any any
DeviceA(config-exp-nacl)# exit
```

(2) Apply the expert extended ACL to a port.

On device A, apply the ACL to the inbound direction of the port connected to the visitor area.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# expert access-group 2700 in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA(config)# show access-lists
expert access-list extended 2700
 10 deny ip any any 192.168.1.0 0.0.0.255 any
 20 deny ip any any host 10.1.1.1 any
 30 permit ip any any any any
```

```
DeviceA(config)# show access-group
expert access-group 2700in
Applied On interface GigabitEthernet 0/2
```

Ping the financial data server from a visitor PC and confirm that the ping operation fails.

Ping the public resource server from a visitor PC and confirm that the ping operation fails.

Ping the internal employee gateway 192.168.1.1 from a visitor PC and confirm that the ping operation fails.

Access the Internet through a visitor PC, for example, access www.baidu.com, and confirm that the home page can be opened.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
expert access-list extended 2700
 10 deny ip any any 10.1.1.0 0.0.0.255 any
 20 deny ip any any host 12.1.1.2 any
 30 permit ip any any any any
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 expert access-group 2700 in
 ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip address 12.1.1.1 255.255.255.0
!
```

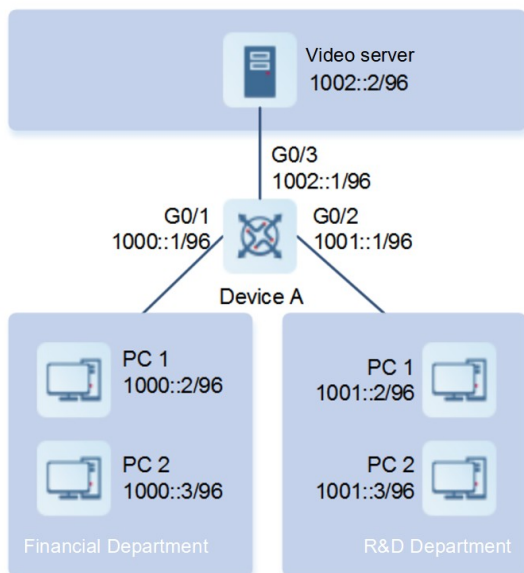

1.10.5 Configuring an IPv6 ACL

1. Requirements

An IPv6 ACL needs to be configured to prevent hosts in the R&D department from accessing the video server.

2. Topology

Figure 1-1 Topology of IPv6 ACL Application Scenario



3. Notes

- On device A, configure an IPv6 ACL and add access rules, including:
 - Prohibiting access to the IPv6 address of the video server.
 - Permitting all the IPv6 packets to pass through.
- On device A, apply the IPv6 ACL to the inbound direction of the port connected to the R&D department.

4. Procedure

(1) Configure an IPv6 ACL and add access rules.

On device A, configure an IPv6 ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ipv6 access-list dev_deny_ipv6video
DeviceA(config-ipv6-nacl)# deny ipv6 any host 1002::2
DeviceA(config-ipv6-nacl)# permit ipv6 any any
DeviceA(config-ipv6-nacl)# exit
```

(2) Apply the IPv6 ACL to a port.

On device A, apply the ACL to the inbound direction of the port connected to the R&D department.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video
in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA(config)# show access-lists

ipv6 access-list dev_deny_ipv6video
10 deny ipv6 any host 200::1
20 permit ipv6 any any

DeviceA(config)# show access-group
ipv6 traffic-filter dev_deny_ipv6video in
Applied On interface GigabitEthernet 0/2
```

Ping the video server from a PC in the R&D department and confirm that the ping operation fails.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ipv6 access-list dev_deny_ipv6video
 10 deny ipv6 any host 1002::2
 20 permit ipv6 any any
!
interface GigabitEthernet 0/1
 no switchport
 ipv6 address 1000::1/96
!
interface GigabitEthernet 0/2
 no switchport
 ipv6 traffic-filter dev_deny_ipv6video in
 ipv6 address 1001::1/96
!
interface GigabitEthernet 0/3
 no switchport
 ipv6 address 1002::1/96
!
```

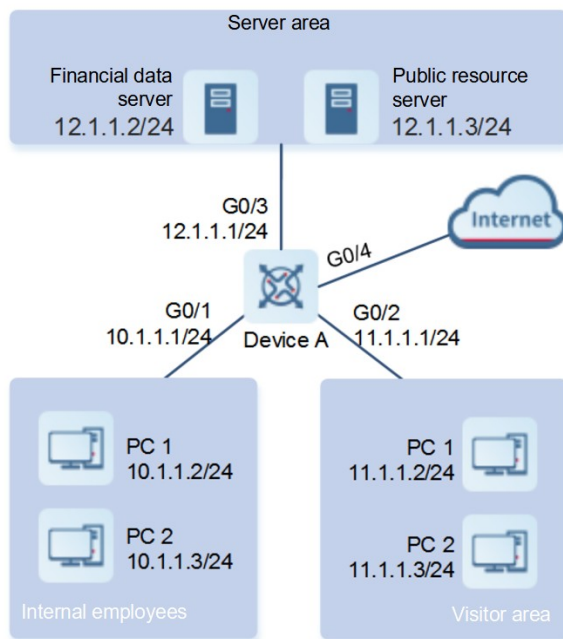
1.10.6 Configuring an ACL80

1. Requirements

An ACL80, namely, an expert advanced ACL needs to be configured to restrict the resources accessible by visitors. Visitors cannot access the PCs of internal employees or the financial data server of the company, but can access the public resource server.

2. Topology

Figure 1-1 Topology of ACL80 Application Scenario



3. Notes

- On device A, configure an expert advanced ACL and add access rules, including:
 - Prohibiting the hosts in the visitor area from sending packets destined to the network segment of internal employees' PCs.
 - Prohibiting visitors from accessing the financial data server.
 - Permitting all the other packets to pass through.
- On device A, apply the ACL to the inbound direction of the port connected to the visitor area.

4. Procedure

(1) Configure an expert advanced ACL and add access rules.

On device A, configure an expert advanced ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# expert access-list advanced acl80-guest
```

```
DeviceA(config-exp-dacl)# deny 0800 FFFF 24 0A0101 FFFFFFFF 42
DeviceA(config-exp-dacl)# deny 0800 FFFF 24 0C010102 FFFFFFFF 42
DeviceA(config-exp-dacl)# permit 0806 FFFF 24
DeviceA(config-exp-dacl)# permit 0800 FFFF 24
DeviceA(config-exp-dacl)# exit
```

(2) Apply the expert advanced ACL to a port.

On device A, apply the ACL80 to the inbound direction of the port connected to the visitor area.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# expert access-group acl80-guest in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA(config)# show access-lists
expert access-list advanced sss
 10 deny 0800 FFFF 24 0A0101 FFFFFFFF 42
 20 deny 0800 FFFF 24 0C010102 FFFFFFFF 42
 30 permit 0806 FFFF 24
 40 permit 0800 FFFF 24

expert access-group acl80-guest in
Applied On interface GigabitEthernet 0/2
```

Ping the financial data server from a visitor PC and confirm that the ping operation fails.

Ping the public resource server from a visitor PC and confirm that the ping operation succeeds.

Ping the internal employee gateway 192.168.1.1 from a visitor PC and confirm that the ping operation fails.

Access the Internet through a visitor PC, for example, access www.baidu.com, and confirm that the home page can be opened.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
expert access-list advanced acl80-guest
 10 deny 0800 FFFF 24 0A0101 FFFFFFFF 42
 20 deny 0800 FFFF 24 0C010102 FFFFFFFF 42
 30 permit 0806 FFFF 24
 40 permit 0800 FFFF 24
!
interface GigabitEthernet 0/1
 no switchport
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
```

```

expert access-group 2700 in
ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
no switchport
ip address 12.1.1.1 255.255.255.0
!

```

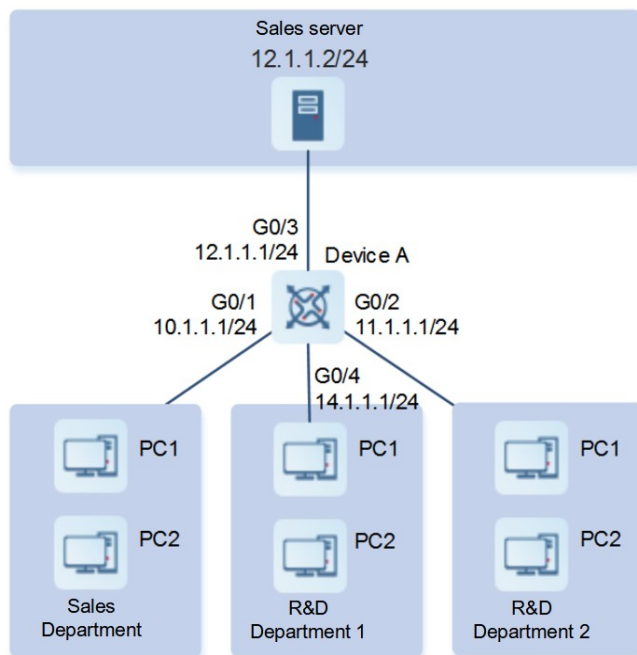
1.10.7 Configuring a Global Security ACL

1. Requirements

The global security ACL function needs to be enabled to prohibit the R&D department from accessing the sales server, but permits the sales department to access it.

2. Topology

Figure 1-1 Topology of Global Security ACL Application Scenario



3. Notes

- On device A, configure an IP extended ACL and add the rule of denying packets with the destination address 12.1.1.2/24.
- Configure the ACL as a global security ACL on device A.
- Configure the port directly connected to the sales department as an excluded port of the global security ACL on device A.

4. Procedure

(1) Configure an IP extended ACL and add access rules.

On device A, configure an IP extended ACL and add access rules.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# ip access-list extended ip_ext_deny_dst_sale_server
DeviceA(config-ext-nacl)# deny ip any host 12.1.1.2
DeviceA(config-ext-nacl)# exit
```

(2) Configure a global security ACL.

Configure the ACL as a global security ACL on device A.

```
DeviceA(config)# ip access-group ip_ext_deny_dst_sale_server in
```

(3) Configure an excluded port of the global security ACL.

Configure the port directly connected to the sales department as an excluded port of the global security ACL on device A.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# no global access-group
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA# show access-lists
ip access-list extended ip_ext_deny_dst_sale_server
 10 deny ip any host 10.1.1.3
DeviceA# show running
.....
!
ip access-group ip_ext_deny_dst_sale_server in
!
.....
!
interface GigabitEthernet 0/1
  no global access-group
!
```

Ping the sales server address from a PC in the sales department, and confirm that the ping operation succeeds.

Ping the sales server address from PCs in R&D departments 1 and 2, and confirm that the ping operation fails.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ip access-list extended ip_ext_deny_dst_sale_server
```

```

10 deny ip any host 12.1.1.2
!
ip access-group ip_ext_deny_dst_sale_server in
!
interface GigabitEthernet 0/1
 no switchport
 no global access-group
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 ip address 11.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/3
 no switchport
 ip address 12.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/4
 no switchport
 ip address 14.1.1.1 255.255.255.0
!

```

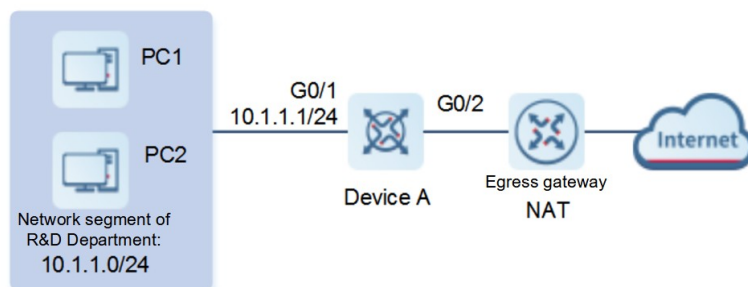
1.10.8 Configuring ACL Rules Based on Time Range

1. Requirements

ACL rules based on time range need to be configured to permit the R&D department to access the Internet only from 12:00 to 13:30 every day.

2. Topology

Figure 1-1 Topology of Time Range-based ACL Rule Application Scenario



3. Notes

- Configure a time range on device A and add the time range entry from 12:00 to 13:30 every day.
- On device A, configure an IP standard ACL and add access rules, including:

- Permitting packets from the source IP network segment 10.1.1.0/24 and associating the rule with the time range named access-internet.
- Denying packets from the source IP network segment 10.1.1.0/24. This rule indicates that the Internet access is rejected beyond the time range.
- Permitting packets from network segment addresses other than the R&D network segment addresses.
- On device A, apply the ACL to the inbound direction of the port connected to the R&D department.

4. Procedure

(1) Configure a time range.

Configure a time range on device A.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# time-range access-internet
DeviceA(config-time-range)# periodic daily 12:00 to 13:30
DeviceA(config-time-range)# exit
```

(2) Configure an IP standard ACL and add access rules.

On device A, configure an IP standard ACL and add access rules.

```
DeviceA(config)# ip access-list standard ip_std_internet_acl
DeviceA(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet
DeviceA(config-std-nacl)# deny 10.1.1.0 0.0.0.255
DeviceA(config-std-nacl)# permit any
DeviceA(config-std-nacl)# exit
```

(3) Apply the IP standard ACL to a port.

On device A, apply the ACL to the inbound direction of the port connected the egress gateway.

```
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip access-group ip_std_internet_acl in
```

5. Verification

Check whether the ACL configuration commands are correct on device A.

```
DeviceA# show time-range

time-range entry: access-internet (inactive)
  periodic Daily 12:00 to 13:30

DeviceA# show access-lists

ip access-list standard ip_std_internet_acl
  10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive)
  20 deny 10.1.1.0 0.0.0.255
  30 permit any

DeviceA# show access-group
```



```
ip access-group ip_std_internet_acl in
Applied On interface GigabitEthernet 0/1
```

During the effective period of the time range (12:00 to 13:30), visit the home page of www.baidu.com from a PC in the R&D department, and confirm that it can be accessed.

During the ineffective period (time beyond 12:00 to 13:30), visit the home page of www.baidu.com from a PC in the R&D department, and confirm that it cannot be accessed.

6. Configuration Files

Device A configuration file

```
hostname DeviceA
!
ip access-list standard ip_std_internet_acl
 10 permit 10.1.1.0 0.0.0.255 time-range access-internet
 20 deny 10.1.1.0 0.0.0.255
 30 permit any
!
time-range access-internet
 periodic daily 12:00 to 13:30
!
interface GigabitEthernet 0/1
 no switchport
 ip access-group ip_std_internet_acl in
 ip address 10.1.1.1 255.255.255.0
!
```