Configuring Access Control List

Information About Access Control List

An Access Control List (ACL) is an ordered set of rules that you can use to filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. You can use ACLs to protect your network and specific hosts from unwanted traffic.

When an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied. If there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied.

Types of ACL

ACL is divided into the following types, based on the purpose of application:

- **Standard ACL**: Defines the rules based on source IP addresses only. Standard ACLs control traffic by comparing the source address of the IP packet to the addresses defined in the ACL.
- **Extended ACL**: Defines the rules based on the source IP address, destination IP address, protocol type, and the protocol attributes of packets.
- **Layer 2 ACL**: Defines the rules based on the source MAC address, destination MAC address, VLAN priority, and Layer 2 protocol type.

Matching Order

An ACL consists of multiple permit or deny rules. The rules may overlap or conflict. In such cases, the matching order decides which rule is executed. ACL supports two matching orders:

- **config**: Matches the ACL rules according to the configuration order.
- **auto**: Matches the ACL rules according to the depth-first rule, wherein the longest subitem in a rule takes priority. The longest subset of a rule is matched first before the rule.

Naming Methods

An ACL is classified into the following types, based on the naming methods:

- **Numbered ACL**: The ACL is identified by the number assigned to it. You can create an ACL and assign a number to it. If you don't specifiy a number, the system assigns a number to the created ACL.

  For a Standard ACL, the numbers range from 1 through 99. You can create upto 99 Standard ACLs.

  For an Extended ACL, the numbers range from 100 through 199. You can create upto 100 Extended ACLs.

  For a Layer 2 ACL, the numbers range from 200 through 299. You can create a maximum of 100 Layer 2 ACLs.

- **Named ACL**: The ACL is identified by the name assigned to it. A named ACL consists of a name and number.

  You can create a maximum of 1000 named ACLs and also define upto 128 subrules for each ACL.

Time Range

A time-based ACL allows for access control based on time. You can create a time range to define specific times of the day and week in order to implement time-based ACLs. A time range is identified by a name and then referenced by a function. Time range can depend on the network access behavior of the users and network congestion condition.

Time range configurations include the absolute time range and periodic time range. A periodic time range configuration is in the form of days of the week. An absolute time range is in the form of start time to the end time.

How to Configure Access Control List

The following sections provide information about configuring Access Control List:

Configuring ACL Matching Order

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**access-list** *access-list* **match-order{ auto | config}** **Example:** `Device(config)#access-list 2 match-order config`	(Optional) Configures the ACL matching order. The default matching order is **config**.

Example Configuration for ACL Matching Order

The following example shows the **config** matching order in a two subitem ACL list.

```
Device#configure terminal
Device(config)#access-list 1 deny any

Device(config)#access-list 1 permit 1.1.1.1 0

Device(config)#show access-list config 1
Standard IP Access List 1, match-order is config, 2 rule:
0  deny    any
permit  1.1.1.1  0.0.0.0
```

The following example shows the **auto** matching order in a two subitem ACL list.

```
Device#configure terminal
Device(config)#access-list 1 match-order auto
Device(config)#access-list 1 deny any
Device(config)#access-list 1 permit 1.1.1.1 0

Device(config)#show access-list config 1
Standard IP Access List 1,  match-order is auto, 2 rule:
0  permit  1.1.1.1  0.0.0.0
1  deny    any
```

Configuring Time Range

You can configure the time range for an ACL either as an absolute time or as a periodic time. Periodic time range is in the form of days of the week. An absolute time range is in the form of start time and end time.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**time-range** *name* **Example:** `Device(config)#time-range timeACL`	Creates a time range and enters the time range configuration mode.
Step 3	**absolute start** *HH:MM:SS YYYY/MM/DD* [**end** *HH:MM:SS YYYY/MM/DD* **Example:** `Device(config-timerange-timeACL)#absolute start 16:00:00 2020/03/30 end 16:00:00 2020/03/31`	Configures an absolute time range. If you do not specify the start date, the time ranges from the earliest time supported by the system to the configured end date. If you do not specify the end date, the time ranges from the configured start date to 2100/12/31 23:59.
Step 4	**periodic** *days-of-the-week HH:MM:SS* **to** [*days-of-the-week*] *HH:MM:SS* **Example:**	Configures a periodic time range.

	Command or Action	Purpose
	`Device(config-timerange-timeACL)#periodic weekdays 8:00:00 to 18:00:00`	
Step 5	**no time-range** [**all** | **name** *name* **Example:** `Device(config)#no time-range all`	(Optional) Removes the specified time range configuration.

Example Configuration for Time Range

The following example configures a time range from 16:00 on March 30, 2020 to 16:00 on March 31, 2020.

```
Device#configure terminal
Device(config)#time-range b
Device(config-timerange-b)#absolute start 16:00:00 2020/03/30 end 16:00:00 2020/03/31
Device(config-timerange-b)#show  time-range name b
Current time is: 10:19:16   2020/03/30  Monday
time-range: b ( Inactive )
absolute:  start  16:00:00  2020/03/30  end  16:00:00  2020/03/31
```

The following example configures a periodic time range, which ranges from 8:00 to 18:00 and Monday to Friday.

```
Device#configure terminal
Device(config)#time-range d
Device(config-timerange-d)#periodic weekdays 8:00:00 to 18:00:00
Device(config-timerange-b)#show time-range name d
Current time is: 10:23:33   2015/03/30  Monday
time-range:d ( Inactive )
periodic:  weekdays 08:00:00  to 18:00:00
```

Configuring Standard ACL

Standard ACLs can be Named ACLs or Numbered ACLs, as described in the following sections.

Configuring a Numbered Standard ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**access-list** *num* {**permit** | **deny** } { *source-IPv4 / IPv6 source-wildcard* | **any** | **ipv6any** } [**time-range** *name*] **Example:** `Device(config)#access-list 4 deny any`	Defines a numbered ACL. The following are the parameters of the command: • **permit** | **deny**:

	Command or Action	Purpose
		Use the keyword **permit** to allow access. Use **deny** not to allow access. • *source-IPv4 / IPv6 source-wildcard* **| any | ipv6any**: Specifies the source address of the ACL rule. *source-IPv4 / IPv6 source-wildcard* specifies the source IP address (IPv4 or IPv6) range of the packet. A *source-wildcard* with a value of zero indicates the host address. **any** specifies any IPv4 source address. **ipv6any** specifies any IPv6 source address. • **time-range** *name*: Specifies the time range in which the ACL rule takes effect.
Step 3	**no access-list** [*number* **| name** *name* **|all**] **Example:** `Device(config)#no access-list 4`	(Optional) Removes the ACL specified. If **all** is specified, removes all the ACLs.

Example Configuration for a Standard ACL

The following example defines a numbered ACL to forbid the packets that have a source address of 10.0.0.1.

```
Device#configure terminal
Device(config)#access-list 1 deny 10.0.0.1 0
```

Configuring a Named Standard ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**access-list standard** *name* **Example:** `Device(config)#access-list standard stdacl`	Defines a Standard ACL based on name and enters the ACL configuration mode.
Step 3	{**permit | deny** } { *source-IPv4 / IPv6 source-wildcard* **| any | ipv6any** } [**time-range** *name*] **Example:**	Configures the ACL rule. The following are the parameters of the command: • **permit | deny**:

	Command or Action	Purpose
	`Device(config-std-nacl-stdacl)#deny ipv6any`	Use the keyword **permit** to allow access. Use **deny** not to allow access. • *source-IPv4 / IPv6 source-wildcard* | **any** | **ipv6any**: Specifies the source address of the ACL rule. *source-IPv4 / IPv6 source-wildcard* specifies the source IP address (IPv4 or IPv6) range of the packet. A *source-wildcard* with a value of zero indicates the host address. **any** specifies any IPv4 source address. **ipv6any** specifies any IPv6 source address. • **time-range** *name*: Specifies the time range in which the ACL rule takes effect.
Step 4	**no access-list** [*number* | **name** *name* | **all**] **Example:** `Device(config)#no access-list name stdacl`	(Optional) Removes the ACL specified.

Example Configuration for a Standard ACL

The following example defines a named ACL to forbid the packets that have a source address of 10.0.0.2.

```
Device#configure terminal
Device(config)#access-list standard stdacl
Device(config-std-nacl-stdacl)#deny 10.0.0.2 0
```

Configuring Extended ACL

Extended ACLs can be Named ACLs or Numbered ACLs, as described in the following sections.

Configuring a Numbered Extended ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**access-list** *num* {**permit** | **deny** } [*protocol*] [**established**] { *source-IPv4 / IPv6 source-wildcard* | **any**	Defines a number-based Extended ACL. The following are the parameters of the command:

	Command or Action	Purpose
	| ipv6any } [*source-port wildcard*] { *dest-IPv4 / IPv6 dest-wildcard* **| any | ipv6any** } [*dest-port wildcard*] [*icmp-type icmp-code*] [*igmp-type*] [**traffic-class** *traffic-class*] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *name*] **Example:** `Device(config)#access-list 102 permit tcp 10.0.0.1 0 ftp any`	• **permit | deny**: Use the keyword **permit** to allow access. Use **deny** not to allow access. • *source-IPv4 / IPv6 source-wildcard* **| any | ipv6any**: Specifies the source address from where the packets originate. *source-IPv4 / IPv6 source-wildcard* specifies the source IP address (IPv4 or IPv6) range of the packet. A *source-wildcard* with a value of zero indicates the host address. **any** specifies any IPv4 source address. **ipv6any** specifies any IPv6 source address. • *protocol*: Specifies the type of IP protocol. It is in the range of 1–255 by number. Select from GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP, and ICMPv6 to specify the protocol by name. • **established**: Defines the SYN flag in TCP. A value 1 indicates that the flag is active. • *dest-IPv4 / IPv6 dest-wildcard* **| any | ipv6any**: Specifies the destination address to which the packets are being sent. *dest-IPv4 / IPv6 dest-wildcard* specifies the destination IP address (IPv4 or IPv6) range of the packet. An IPv4 address is in dotted decimal notation. An IPv6 address is in hexadecimal notation. A *dest-wildcard* with a value of zero indicates the host address. **any** specifies any IPv4 source address. **ipv6any** specifies any IPv6 destination address. • *source-port / dest-port wildcard*: Specifies the TCP or UDP source and destination port numbers. • *icmp-type icmp-code*: Specifies the type of ICMP protocol packet. It is valid only when protocol is configured as **icmp** or **icmpv6**.

	Command or Action	Purpose
		• *igmp-type*: Specifies the type of IGMP protocol packet. It is valid only when protocol is configured as **igmp**. • **traffic-class**: Specifies the traffic class for IPv6. • **precedence**: Specifies the precedence priority. IP precedence ranges from 0 through 7. • **tos**: Specifies the Type of Service (ToS) priority. The values range from 0 through 15. • **dscp**: Specifies the Differentiated Services Code Point (DSCP) priority value. • **fragments**: Specifies that the ACL rule is valid for nonfirst fragmented packets. This helps prevent fragment packet attacks. • **time-range** *name*: Specifies the time range in which the ACL rule takes effect.
Step 3	**no access-list** [*number* | **all**] **Example:** `Device(config)#no access-list 102`	(Optional) Removes the ACL specified.

Example Configuration for an Extended ACL

The following example defines a number-based Extended ACL to deny FTP packets that have a source address of 10.0.0.1.

```
Device#configure terminal
Device(config)#access-list 100 deny tcp 10.0.0.1 0 ftp any
```

Configuring a Named Extended ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**access-list extended** *name* **Example:** `Device(config)#access-list extended extacl`	Defines a name-based Extended ACLand enters the ACL configuration mode.
Step 3	{ **permit** | **deny** } [*protocol*] [**established**] { *source-IPv4 / IPv6 source-wildcard* | **any** | **ipv6any** } [*source-port wildcard*] { *dest-IPv4 / IPv6 dest-wildcard* | **any** | **ipv6any** } [*dest-port wildcard*] [*icmp-type icmp-code*] [*igmp-type*] [**traffic-class** *traffic-class*] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragments**] [**time-range** *name*] **Example:** `Device(config-ext-nacl-extacl)#deny tcp 10.0.0.1 0 ftp any`	Defines a name-based Extended ACL. The following are the parameters of the command: • **permit | deny**: Use the keyword **permit** to allow access. Use **deny** not to allow access. • *source-IPv4 / IPv6 source-wildcard* **| any | ipv6any**: Specifies the source address from where the packets originate. *source-IPv4 / IPv6 source-wildcard* specifies the source IP address (IPv4 or IPv6) range of the packet. A *source-wildcard* with a value of zero indicates the host address. **any** specifies any IPv4 source address. **ipv6any** specifies any IPv6 source address. • *protocol*: Specifies the type of IP protocol. It is in the range of 1–255 by number. Select from GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP, and ICMPv6 to specify the protocol by name. • **established**: Defines the SYN flag in TCP. A value 1 indicates that the flag is active. • *dest-IPv4 / IPv6 dest-wildcard* **| any | ipv6any**: Specifies the destination address to which the packets are being sent. *dest-IPv4 / IPv6 dest-wildcard* specifies the destination IP address (IPv4 or IPv6) range of the

	Command or Action	Purpose
		packet. An IPv4 address is in dotted decimal notation. An IPv6 address is in hexadecimal notation. A *dest-wildcard* with a value of zero indicates the host address. **any** specifies any IPv4 source address. **ipv6any** specifies any IPv6 destination address. • *source-port / dest-port wildcard*: Specifies the TCP or UDP source and destination port numbers. • *icmp-type icmp-code*: Specifies the type of ICMP protocol packet. It is valid only when protocol is configured as **icmp** or **icmpv6**. • *igmp-type*: Specifies the type of IGMP protocol packet. It is valid only when protocol is configured as **igmp**. • **traffic-class**: Specifies the traffic class for IPv6. • **precedence**: Specifies the precedence priority. IP precedence ranges from 0 through 7. • **tos**: Specifies the Type of Service (ToS) priority. The values range from 0 through 15. • **dscp**: Specifies the Differentiated Services Code Point (DSCP) priority value. • **fragments**: Specifies that the ACL rule is valid for nonfirst fragmented packets. This helps prevent fragment packet attacks. • **time-range** *name*: Specifies the time range in which the ACL rule takes effect.
Step 4	**no access-list** [*name* | **all**] **Example:** `Device(config)#no access-list all`	(Optional) Removes the ACL specified.

Configure an Extended ACL

The following example defines a name-based Extended ACL to deny FTP packets that have a source address of 10.0.0.2.

```
Device#configure terminal

Device(config)#access-list extended extacl
Device(config)#deny tcp 10.0.0.2 0 ftp any
```

Configuring Layer 2 ACL

Layer 2 ACLs establish rules based on Layer 2 information like MAC address, VLAN priorities, and Layer 2 protocol types. Layer 2 ACLs can be name-based or number-based.

Configuring a Numbered Layer 2 ACL

SUMMARY STEPS

1. **configure terminal**
2. **access-list** *num* {**permit** | **deny** } [*protocol*] [**cos** *vlan-pri*] **ingress**{ { [**inner-vid***vid*] [*start-vlan-id end-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface-number*] } | **any** } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-number* | **cpu**] } | **any** } [**time-range** *name*]
3. **no access-list** [*number* | **all**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**access-list** *num* {**permit**	**deny** } [*protocol*] [**cos** *vlan-pri*] **ingress**{ { [**inner-vid***vid*] [*start-vlan-id end-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface-number*] }	**any** } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-number*	**cpu**] }	**any** } [**time-range** *name*] **Example:** `Device(config)#access-list 202 deny arp ingress 00:00:00:00:00:01 0 egress`	Defines a number-based Layer 2 ACL. The following are the parameters of the command: • **permit**	**deny**: Use the keyword **permit** to allow access. Use **deny** not to allow access. • *protocol* : Specifies the type of protocol packet carried by the Ethernet frame. In hexadecimal notation, the range is 0 through FFFF. It is optional ion case of ARP, IP, RARP. • *protocol*: Specifies the type of IP protocol.

	Command or Action	Purpose
		It is in the range of 1–255 by number. Select from GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP, and ICMPv6 to specify the protocol by name. • **cos**: Defines the priority of the VLAN tag. • **ingress** : Specifies the rule for the incoming packets at the ingress port. • **inner-vid**: Specifies the inner VLAN ID of a double-tagged packet. • *start-vlan-id end-vlan-id*: Specifies the range of VLANs. For a double-tagged packet, it is the VLAN ID of the outer tag. • *source-mac-addr source-mac-wildcard*: Specifies the source MAC address options. *source-mac-wildcard* indicates the source MAC range. • **interface** *interface-num*: Specifies the physical port number. It can be either the ingress port or the egress port. • **CPU**: Indicates that the data will be forwarded to the CPU. • **any**: Specifies any address which can be at ingress or egress directions. • **time-range** *name*: Specifies the time range in which the ACL rule takes effect.
Step 3	**no access-list** [*number* | **all**] **Example:** `Device(config)#no access-list 102`	(Optional) Removes the ACL specified.

Example Configuration for a number-based Layer 2 ACL

The following example defines a number-based Layer 2 ACL to disable the ARP packet whose source MAC address is 00: 00: 00: 00: 00: 01.

```
Device#configure terminal
Device(config)#access-list 200 deny arp ingress 00:00:00:00:00:01 0 egress any
```

Configuring a Named Layer 2 ACL

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**access-list link** *name* **Example:** `Device(config)#access-list link layer2acl`	Defines a Layer 2 ACL and enters the ACL configuration mode.
Step 3	{**permit** | **deny** } [*protocol*] [**cos** *vlan-pri*] **ingress**{ { [**inner-vid***vid*] [*start-vlan-id end-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface-number*] }| **any** } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-number* | **cpu**] } | **any** } [**time-range** *name*] **Example:** `Device(config-link-nacl-layer2acl)#deny arp ingress 00:00:00:00:00:01 0 egress any`	Defines a Layer 2 ACL. The following are the parameters of the command: • **permit | deny**: Use the keyword **permit** to allow access. Use **deny** not to allow access. • *protocol* : Specifies the type of protocol packet carried by the Ethernet frame. In hexadecimal notation, the range is 0 through FFFF. It is optional in case of ARP, IP, RARP protocols. • **cos**: Defines the priority of the VLAN tag. • **ingress** : Specifies the rule for the incoming packets at the ingress port. • **inner-vid**: Specifies the inner VLAN ID of a double-tagged packet. • *start-vlan-id end-vlan-id*: Specifies the range of VLANs.

	Command or Action	Purpose
		For a double-tagged packet, it is the VLAN ID of the outer tag. • *source-mac-addr source-mac-wildcard*: Specifies the source MAC address options. *source-mac-wildcard* indicates the source MAC range. • **interface** *interface-num*: Specifies the physical port number. It can be either the ingress port or the egress port. • **CPU**: Indicates that the data is forwarded to the CPU. • **any**: Specifies any address which can be at ingress or egress directions. • **time-range** *name*: Specifies the time range in which the ACL rule takes effect.
Step 4	**no access-list** [*name* | **all**] **Example:** `Device(config)#no access-list all`	(Optional) Removes the ACL specified.

Example Configuration for a number-based Layer 2 ACL

The following example defines a name-based Layer 2 ACL to disable the ARP packet whose source MAC address is 00: 00: 00: 00: 00: 02.

```
Device#configure terminal

Device(config)#access-list link layer2acl
Device(config-link-nacl-layer2acl)#deny arp ingress 00:00:00:00:00:02 0 egress any
```

Activating an Access Control List

You have to activate an ACL for it to be effective. ACL follows the rule "First Activation, First Served".

Before you begin

To activate an ACL, ensure that the ACL is defined.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#configure terminal`	Enters the global configuration mode.
Step 2	**access-group** [**ip-group** *name* | *num*] [**link-group** *name* | *num*] [**subitem** *num*] **Example:** `Device(config)#access-group ip-group 1 subitem 1`	Activates the specified ACL.
Step 3	**no access-group** [**ip-group** *name* | *num*] [**link-group** *name* | *num*] [**subitem** *num*] **Example:** `Device(config)#no access-group ip-group 1 subitem 1`	Deactivates the specified ACL.
Step 4	**no access-group all** **Example:** `Device(config)#no access-group all`	Deactivates all the ACLs.

Configuration Examples for Activating an ACL

The following example configures an ACL numbered 1 and activates it.

```
Device#configure terminal
Device(config)#access-list 1 deny any

Device(config)#access-list 1 permit 1.1.1.1 0
Device(config)#show access-list config 1
Standard IP Access List 1, match-order is config, 2 rule:
  0  deny    any
permit  1.1.1.1  0.0.0.0


Device(config)#access-group ip-group 1 subitem 1

Device(config)#access-group ip-group 1 subitem 0
```

In this case, because first activation takes precedence, the device allows only those packets with a source IP address of 1.1.1.1 to pass through.

The following example configures a Standard ACL with match-order **auto** and activates it.

```
Device#configure terminal
Device(config)#access-list 1 match-order auto
Device(config)#access-list 1 deny any
Device(config)#access-list 1 permit 1.1.1.1 0
Device(config)#show access-list config 1
Standard IP Access List 1, match-order is auto, 2 rule:
0  permit  1.1.1.1  0.0.0.0
1  deny    any
```

```
Device(config)#access-group ip-group 1 subitem 0
Device(config)#access-group ip-group 1 subitem 1
```

In this case, because first activation takes precedence, the device allows only those packets that have a source IP address 1.1.1.1 to pass through.

The following example configures multiple ACLs and activates them to achieve IP, MAC, and port binding.

```
Device#configure terminal

Device(config)#access-list 1 permit 1.1.1.1 0
Device(config)#access-list 200 permit ingress 00:00:00:00:00:01 0 interface ethernet 0/1
egress any
Device(config)#access-group ip-group 1 link-group 200
```

Verifying Access Control List Configurations

After you have configured ACL for your devices, use the following commands to view the configurations.

Table 1: Show commands to Verify ACL Configurations

Command	Purpose
show access-list config statistic	Displays ACLstatistics. You can execute the command in any mode.
show access-list config { **all** | *num* | **name** *name* }	Displays the ACLs. You can execute the command in any mode.
show access-list runtime statistic	Displays the number of activated ACLs. You can execute the command in any mode.
show access-list runtime { **all** | *num* | **name** *name* }	Displays details of the activated ACLs. You can execute the command in any mode.