FSOS

ACL Configuration

Contents

1. ACL Configuring.....3
1.1 Brief Introduction to ACL..... 3
1.1.1 Configuring Match Order..... 3
1.1.2 Switch Support ACL..... 4
1.2 Configuring Time Range.....4
1.2.1 Configuration Procedure.....4
1.2.2 Configuration Examples.....5
1.3 Configuring a Basic ACL.....5
1.3.1 Configuration Procedure.....6
1.3.2 Configuration Examples.....6
1.4 Define Extended ACL.....6
1.4.1 Configuration Procedure.....6
1.4.2 Configuration Procedure.....8
1.5 Define Layer 2 ACL..... 8
1.5.1 Configuring Layer 2 ACL.....8
1.5.2 Configuration Examples.....9
1.6 Activate ACL..... 9
1.6.1 Configuration Examples..... 10
1.6.2 Activate ACL successfully .Active ACL Binding.....10
1.7 Displaying and Debugging ACL.....10

1. ACL Configuring

1.1 Brief Introduction to ACL

As network scale and network traffic are increasingly growing, network security and bandwidth allocation become more and more critical to network management. Packet filtering can be used to efficiently prevent illegal users from accessing networks and to control network traffic and save network resources. Access control lists (ACL) are often used to filter packets with configured matching rules.

ACLs are sets of rules (or sets of permit or deny statements) that decide what packets can pass and what should be rejected based on matching criteria such as source MAC address, destination MAC address, source IP address, destination IP address, and port number.

When an ACL is assigned to a piece of hardware and referenced by a QoS policy for traffic classification, the switch does not take action according to the traffic behavior definition on a packet that does not match the ACL.

ACL according to application identified by ACL numbers, fall into three categories,

- Basic ACL: Source IP address
- Extended ACL: Source IP address, destination IP address, protocol carried on IP, and other Layer 3 or Layer 4 protocol header information
- Layer 2 ACL: Layer 2 protocol header fields such as source MAC address, destination MAC address, 802.1p priority, and link layer protocol type

1.1.1 Configuring Match Order

An ACL consists of multiple rules, each of which specifies different matching criteria. These criteria may have overlapping or conflicting parts. This is where the order in which a packet is matched against the rules comes to rescue.

Two match orders are available for ACLs:

- config: where packets are compared against ACL rules in the order in which they are configured.
- auto: where depth-first match is performed. The term depth-first match has different meanings for different types of ACLs. Depth-first match for a basic ACL

  For example, now configuring 2 types of ACL as below:

  Switch(config)#access-list 1 deny any

  Config ACL subitem successfully.

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

  Config ACL subitem successfully.
- If it is the configuration mode, sub-item 0 is the first command. You can see as below configuration:

  Switch(config)#show access-list config 1

  Standard IP Access List 1, match-order is config, 2 rule:

  0 deny any

1 permit 1.1.1.1 0.0.0.0

- If it is the auto mode, sub-item 0 is the longest ACL match rule. You can see as below configuration:

Switch(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

Notes, ACL must enable. Switches must obey “first enable then active. Please refer to Chapter 1.6 for detailed configuration.

1.1.2 Switch Support ACL

Switch support ACL as below:

- Basic ACL
- Extended ACL
- Layer 2 AC

1.2 Configuring Time Range

There are two kinds of configuration: configure absolute time range and periodic time range. Configuring absolute is in the form of year, month, date, hour and minute. Configuring periodic time range is in the form of day of week, hour and minute.

1.2.1 Configuration Procedure

Table 1-1 Configuration procedure

Command	Operation	remark
Enter global configuration mode	**configure terminal**	-
new build time range and enter time range mode	**time-range** *name*	-
Configure absolute start	**absolute start** *HH:MM:SS YYYY/MM/DD* [**end** *HH:MM:SS YYYY/MM/DD*]	required
Configure periodic start	**periodic** *days-of-the-week hh:mm:ss* **to** [*day-of-the-week*] *hh:mm:ss*	

Note that:
Periodic time range created using the time-range time-name start-time to end-time days command. A time range thus created recurs periodically on the day or days of the week.
Absolute time range created using the time-range time-name {from time1 date1 [to time2 date2] | to time2 date2 } command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the time-range test from 00:00 01/01/2004 to 23:59 12/31/2004 command.
Compound time range created using the time-range time-name start-time to

end-time days { from time1 date1 [to time2 date2] | to time2 date2 } command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the time-range test 12:00 to 14:00 Wednesday from 00:00 01/01/2004 to 23:59 12/31/2004 command.

You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.

With no start time specified, the time range is from the earliest time that the system can express (that is, 00:00 01/01/1970) to the end time. With no end time specified, the time range is from the time the configuration takes effect to the latest time that the system can express (that is, 24:00 12/31/2100).

Up to 256 time ranges can be defined.

1.2.2 Configuration Examples

1. Create an absolute time range from 16:00, Jan 3, 2009 to 16:00, Jan 5, 2009

```
Switch#configure terminal
Switch(config)#time-range b
Config time range successfully.
Switch(config-timerange-b)#absolute start 16:00:00 2009/1/3 end 16:00:00 2009/1/5
Config absolute range successfully .
Switch(config-timerange-b)#show time-range name b
Current time is: 02:46:43      2009/01/31      Saturday

time-range: b ( Inactive )
absolute:  start  16:00:00  2009/01/03  end  16:00:00  2009/01/05
```

2. Create a periodic time range that is active from 8:00 to 18:00 every working day.

```
Switch#configure terminal
Switch(config)#time-range b
Config time range successfully.
Switch(config-timerange-b)#periodic weekdays 8:00:00 to 18:00:00
Config periodic range successfully .
Switch(config-timerange-b)#show time-range name b
Current time is: 02:47:56      2009/01/31    Saturday

time-range: b ( Inactive )
periodic:   weekdays 08:00   to              18:00
```

1.3 Configuring a Basic ACL

Basic ACLs filter packets based on source IP address. They are numbered in the range 1 to 99. At most 99 ACL with number mark and at most 1000 ACL with name mark. At most 128 rules for each ACL at the same time. If you want to reference a time range to a rule, define it with the time-range command first.

1.3.1 Configuration Procedure

Follow these steps to configure a basic ACL

Table 1-2 Configure basic ACL based on digital identification

Command	Operation	remark
Enter global configuration mode	**configure terminal**	-
Define sub-item match rule	**access-list** *num* **match-order** { **config** | **auto** }	optional by default ,system is config
Define basic ACL	**access-list** *num* { **permit** | **deny** } { *source-IPv4/v6 source-wildcard* | **any** | **ipv6any** } [**time-range** *name*]	required

Table 1-3 Configure basic ACL based on name identification

Command	Operation	remark
Enter global configuration mode	**configure terminal**	-
Define sub-item match rule	**access-list standard** *name* **match-order** { **config** | **auto** }	optional by default ,system is config
Define basic ACL and enter configuration mode	**access-list standard** *name*	required
Configure ACL rule	{ **permit** | **deny** } { *source-IPv4/v6 source-wildcard* | **any** | **ipv6any** } [**time-range** *name*]	required

1.3.2 Configuration Examples

!Define a basic ACL with number mark to deny packet with source IP 10.0.0.1
Switch#configure terminal
Switch(config)#access-list 1 deny 10.0.0.1 0

!Define a basic ACL with name mark to deny packet with source IP 10.0.0.2
Switch#configure terminal
Switch(config)#access-list standard stdacl
Switch(config-std-nacl-stdacl)#deny 10.0.0.2 0

1.4 Define Extended ACL

Switch can define at most 100 extended ACL with the number ID (the number is in the range of 100 to 199), at most 1000 extended ACL with the name ID. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID).

1.4.1 Configuration Procedure

Follow these steps to configure a extended ACL

Table 1-4 Configure extended ACL based on digital identification

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Define sub-item match rule	**access-list** *num* **match-order** { **config** | **auto** }	optional by default ,system is config
Define extended ACL	**access-list** *num* { **permit** | **deny** } [*protocol*] [**established**] { *source-IPv4/v6 source-wildcard* | **any** | **ipv6any** } [*port* [*portmask*]] { *dest-IPv4/v6 dest-wildcard* | **any** | **ipv6any** } [*port* [*portmask*]] { [**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*] } [**time-range** *name*]	required

Table 1-5 Configure extended ACL based on name identification

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Define subitem match rule	**access-list extended** *name* **match-order** { **config** | **auto** }	optional by default ,system is config
Define extended ACL and enter configuration mode	**access-list extended** *name*	required
Configure ACL rule	{ **permit** | **deny** } [*protocol*] [**established**] { *source-IPv4/v6 source-wildcard* | **any** | **ipv6any** } [*port* [*portmask*]] { *dest-IPv4/v6 dest-wildcard* | **any** | **ipv6any** } [*port* [*portmask*]] { [**precedence** *precedence*] [**tos** *tos*] | [**dscp** *dscp*] } [**time-range** *name*]	required

Detailed parameters of extended ACL as below Table 1-6:

Parameters	Function	Remark
protocol	IP protocol type carried	A number in the range of 1 to 255
		Represented by name, you can select GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP
{ *sour-address*	ACL rules specified the source address information	sour-address sour-wildcard used to determine the packet's source IP address. Dotted decimal notation;
sour-wildcard|**any** }		sour-wildcard of 0 means that the host address

		any source address.
{ *dest-addr*	The purpose of ACL rules specified address information	dest-addr dest-wildcard used to determine the packet destination address, in dotted decimal notation; dest-wildcard is 0, the host address
dest-wildcard| **any**}		Any is any destination address.
port	TCP / UDP port number	——
precedence *precedence*	priority precedence message	IP precedence values range from 0 to 7
tos *tos*	tos priority packets	ToS priority ranges from 0 to 15
dscp *dscp*	DSCP priority	Rule applies only to non-first fragment packet effective
	Level ranges from 0 to 63	
	fragment fragmentation information	
time-range *name*	Create a time range	——

1.4.2 Configuration Procedure

!Create extended ACL based on digital identification to deny the FTP packets with source address 10.0.0.1 .
Switch#configure terminal
Switch(config)#access-list 100 deny tcp 10.0.0.1 0 ftp any
!Create extended ACL based on name identification to deny the FTP packets with source address 10.0.0.1.
Switch#configure terminal
Switch (config)#access-list extended extacl
Switch(config-ext-nacl-extacl)#deny tcp 10.0.0.2 0 ftp any

1.5 Define Layer 2 ACL

Switch can define at most 100 layer 2 ACL with the number ID (the number is in the range of 200 to 299), at most 1000 layer 2 ACL with the name ID. It can define 128 sub-rules for an ACL (this rule can suit both ACL with name ID and number ID). Layer 2 ACL only classifies data packet according to the source MAC address, source VLAN ID, layer protocol type, layer packet received and retransmission interface and destination MAC address of layer 2 frame head of data packet and analyze the matching data packet.

1.5.1 Configuring Layer 2 ACL

Follow these steps to configure a Layer 2 ACL

Table 1-7 Configure Layer 2 ACL based on digital identification

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Define sub-item match rule	**access-list** *num* **match-order** { **config** | **auto** }	optional by default ,system is config
Define Layer 2 ACL	**access-list** *num* { **permit** | **deny** } [*protocol*] [**cos** *vlan-pri*] **ingress** { { [*source-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface-num*] } | **any** } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-num* | **cpu**] } | **any** } [**time-range** *name*]	required

Table 1-8 Configure Layer 2 ACL based on name identification

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Define sub-item match rule	**access-list link** *name* **match-order** { **config** | **auto** }	optional by default ,system is config
Define Layer 2 ACL and enter configuration mode	**access-list link** *name*	required
Configure ACL rule	{ **permit** | **deny** } [*protocol*] [**cos** *vlan-pri*] **ingress** { { [*source-vlan-id*] [*source-mac-addr source-mac-wildcard*] [**interface** *interface- num*] } | **any** } **egress** { { [*dest-mac-addr dest-mac-wildcard*] [**interface** *interface-num* | **cpu**] } | **any** } [**time-range** *name*]	required

1.5.2 Configuration Examples

!Create Layer 2 ACL based on digital identification to deny the MAC with ARP address 00:00:00:00:00:01.

Switch#configure terminal

Switch(config)#access-list 200 deny arp ingress 00:00:00:00:00:01 0 egress any

!Create Layer 2 ACL based on name identification to deny the MAC with ARP address 00:00:00:00:00:02.

Switch#configure terminal

Switch(config)#access-list link lnkacl

Switch (config-link-nacl-lnkacl)#deny arp ingress 00:00:00:00:00:02 0 egress any

1.6 Activate ACL

Switch obey the rule of "**First enable then active**"

Table 1-9 Activate ACL

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Active ACL	**access-group [ip-group** *name*|*num*] **[subitem** *num*] **[link-group** *name*|*num*] **[subitem** *num*]	required

1.6.1 Configuration Examples

Switches only permit with source IP address 1.1.1.1

!Before configuration

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

!Configuration steps

Switch(config)#access-group ip-group 1
Activate ACL successfully .

!Before configuration

Switch(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

!Configuration steps

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

Activate ACL successfully .

Switch(config)#access-group ip-group 1 subitem 0

Activate ACL successfully .

1.6.2 Activate ACL successfully .Active ACL Binding

IP+MAC+Port binds through ACL binding active.

!Configuration request

MAC is 00:00:00:00:00:01, IP address of 1.1.1.1 the user can only enter from e0/0/1 mouth.

!Configuration steps

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

1.7 Displaying and Debugging ACL

After finishing above configuration, you can see configuration as below commands.

Table 1-10 Display and debug ACL

Command	Operation	Remark

Display ACL statistics	**show access-list config statistic**	perform either of the commands
Display ACL configuration	**show access-list config {all|***num***|name** *name***}**	
Display ACL	**show access-list runtime {all|***num***|name** *name***}**	