Edge-corE

Powered by Accton

ES4704(10)BD

QoS、PBR and Security

Management Guide

www.edge-core.com

Content

Chapter 1 QoS And PBR Configuration

1.1 QoS Configuration

1.1.1 Introduction to QoS

QoS (Quality of Service) is a set of capabilities that allow you to create differentiated services for network traffic, thereby providing better service for selected network traffic. QoS is a guarantee for service quality of consistent and predictable data transfer service to fulfill program requirements. QoS cannot generate extra bandwidth but provides more effective bandwidth management according to the application requirement and network management policy.

1.1.1.1 QoS Terms

CoS: Class of Service, the classification information carried by Layer 2 802.1Q frames, taking 3 bits of the Tag field in frame header, is called user priority level in the range of 0 to 7.

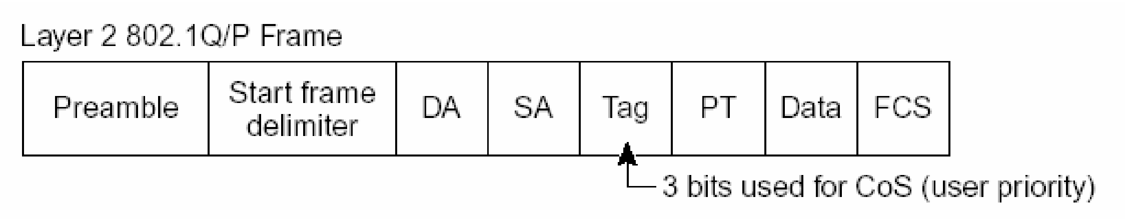


Fig 1-1 CoS priority

ToS: Type of Service, a one-byte field carried in Layer 3 IPv4 packet header to symbolize the service type of IP packets. Among ToS field can be IP Precedence value or DSCP value.

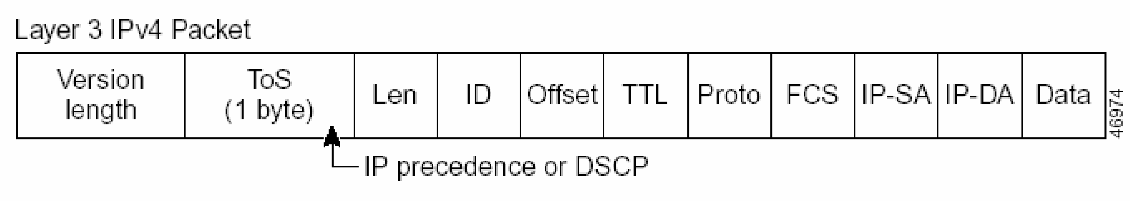


Fig 1-2 ToS priority

IP Precedence: IP priority.Classification information carried in Layer 3 IP packet header, occupying 3 bits, in the range of 0 to 7.

DSCP: Differentiated Services Code Point, classification information carried in Layer 3 IP packet header, occupying 6 bits, in the range of 0 to 63, and is downward compatible with IP Precedence.

DSCP-inside: The switch-inside priority configuration, be used to partition priority for the switch-inside data, range from 0 to 63.

Classification: The entry action of QoS, classifying packet traffic according to the classification information carried in the packet and ACLs.

Policing: Ingress action of QoS that lays down the policing policy and manages the classified packets.

Remark: Ingress action of QoS, perform allowing, degrading or discarding operations to packets according to the policing policies.

Queuing: Egress QoS action. Put the packets to appropriate egress queues according to the packet CoS value.

Scheduling: QoS egress action. Configure the weight for eight egress queues WRR (Weighted Round Robin).

In-Profile: Traffic within the QoS policing policy range (bandwidth or burst value) is called “In-Profile".

Out-of-Profile: Traffic out the QoS policing policy range (bandwidth or burst value) is called “Out-of-Profile".

1.1.1.2 QoS Implementation

To implement Layer 3 switch software QoS, a general, mature reference model should be given. QoS can not create new bandwidth, but can maximize the adjustment and configuration for the current bandwidth resource. Fully implemented QoS can achieve complete management over the network traffic. The following is as accurate as possible a description of QoS.

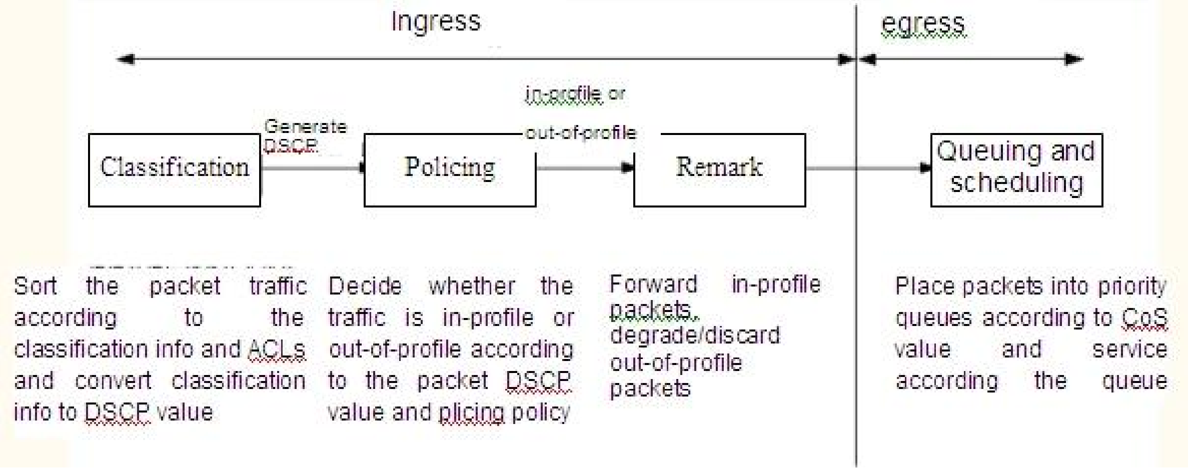
The data transfer specifications of IP cover only addresses and services of source and destination, and ensure correct packet transmission using OSI layer 4 or above protocols such as TCP. However, rather than provide a mechanism for providing and protecting packet transmission bandwidth, IP provide bandwidth service by the best effort. This is acceptable for services like Mail and FTP, but for increasing multimedia business data and e-business data transmission, this best effort method cannot satisfy the bandwidth and low-lag requirement.

Based on differentiated service, QoS specifies a priority for each packet at the ingress. The classification information is carried in Layer 3 IP packet header or Layer 2 802.1Q frame header. QoS provides same service to packets of the same priority, while offers different operations for packets of different priority. QoS-enabled switch or router can provide different bandwidth according to the packet classification information, and can remark on the classification information according to the policing policies configured, and may discard some low priority packets in case of bandwidth shortage.

If devices of each hop in a network support differentiated service, an end-to-end QoS solution can be created. QoS configuration is flexible, the complexity or simplicity depends on the network topology and devices and analysis to incoming/outgoing traffic.

1.1.1.3 Basic QoS Model

The basic QoS consists of five parts: Classification, Policing, Remark, Queuing and Scheduling, where classification, policing and remark are sequential ingress actions, and Queuing and Scheduling are QoS egress actions.



Sort the packet traffic according to the classification info and ACLs and convert classification info to DSCP value

Decide whether the traffic is in-profile or out-of-profile according to the packet DSCP value and plicing policy

Forward in-profile packets, degrade/discard out-of-profile packets

Place packets into priority queues according to CoS value and service according the queue

Fig 1-3 Basic QoS Model

Classification: Classify traffic according to packet classification information and generate internal DSCP value based on the classification information. For different packet types and switch configurations, classification is performed differently; the flowchart below explains this in detail.

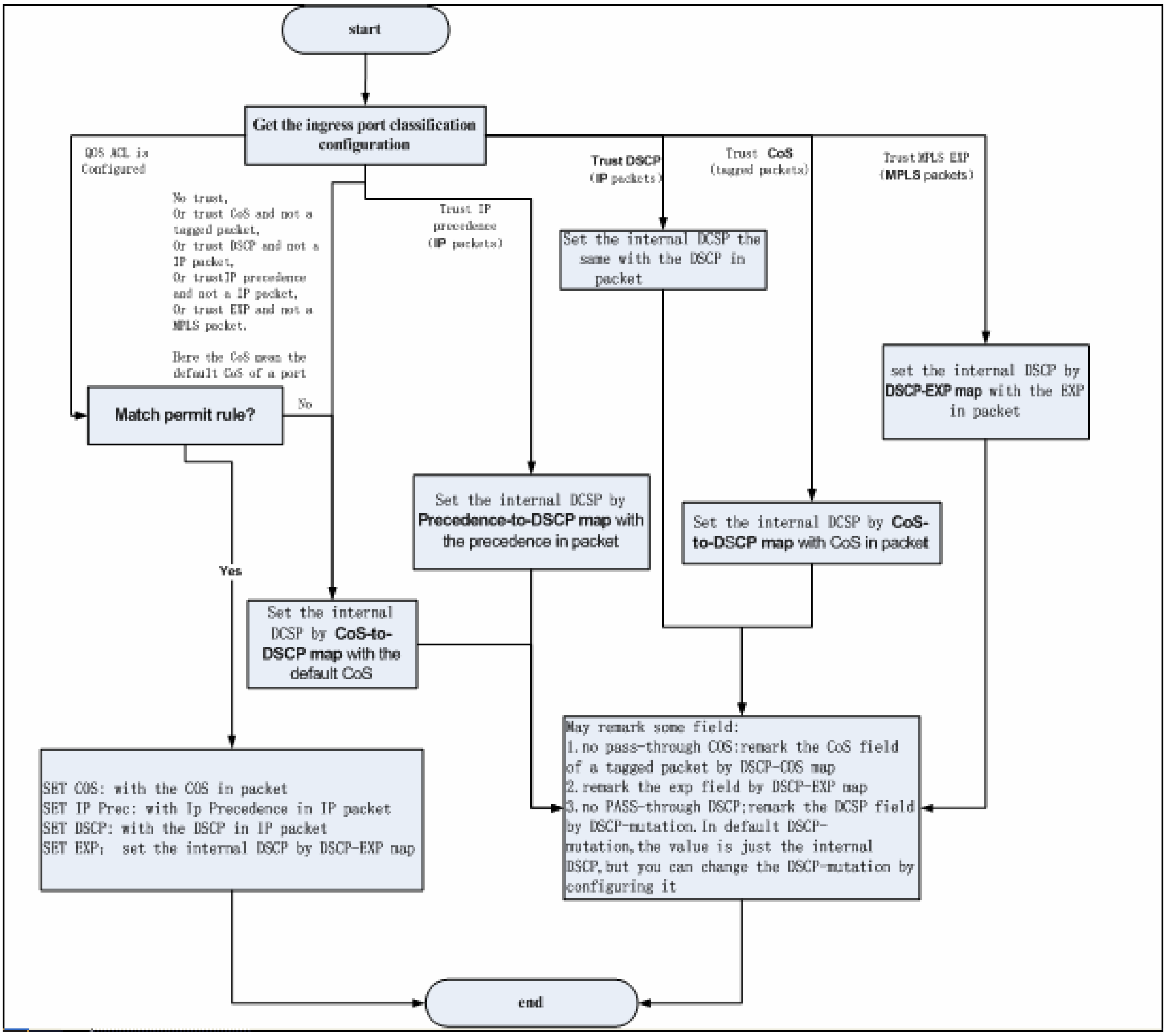

start
Get the ingress port classification configuration
QOS ACL is Configured
No trust,
Or trust CoS and not a tagged packet,
Or trust DSCP and not a IP packet,
Or trustIP precedence and not a IP packet,
Or trust EXP and not a MPLS packet.
Here the CoS mean the default CoS of a port
Trust IP precedence (IP packets)
Trust DSCP (IP packets)
Trust CoS (tagged packets)
Trust MPLS EXP (MPLS packets)
Set the internal DCSP the same with the DSCP in packet
set the internal DSCP by DSCP-EXP map with the EXP in packet
Match permit rule?
No
Set the internal DCSP by Precedence-to-DSCP map with the precedence in packet
Set the internal DCSP by CoS-to-DSCP map with CoS in packet
Yes
Set the internal DCSP by CoS-to-DSCP map with the default CoS
May remark some field:
1.no pass-through COS:remark the CoS field of a tagged packet by DSCP-COS map
2.remark the exp field by DSCP-EXP map
3.no PASS-through DSCP;remark the DCSP field by DSCP-mutation.In default DSCP-mutation,the value is just the internal DSCP,but you can change the DSCP-mutation by configuring it
SET COS: with the COS in packet
SET IP Prec: with Ip Precedence in IP packet
SET DSCP: with the DSCP in IP packet
SET EXP: set the internal DSCP by DSCP-EXP map
end

Fig 1-4 Classification process

Policing and remark: Each packet in classified ingress traffic is assigned an internal DSCP value and can be policed and remarked.

Policing can be performed based on DSCP value to configure different policies that allocate bandwidth to classified traffic. If the traffic exceeds the bandwidth set in the policy (out-of-profile), the out of profile traffic can be allowed, discarded or remarked. Remarking uses a new DSCP value of lower priority to replace the original higher level DSCP value in the packet; this is also called “marking down”. The following flowchart describes the operations during policing and remarking.

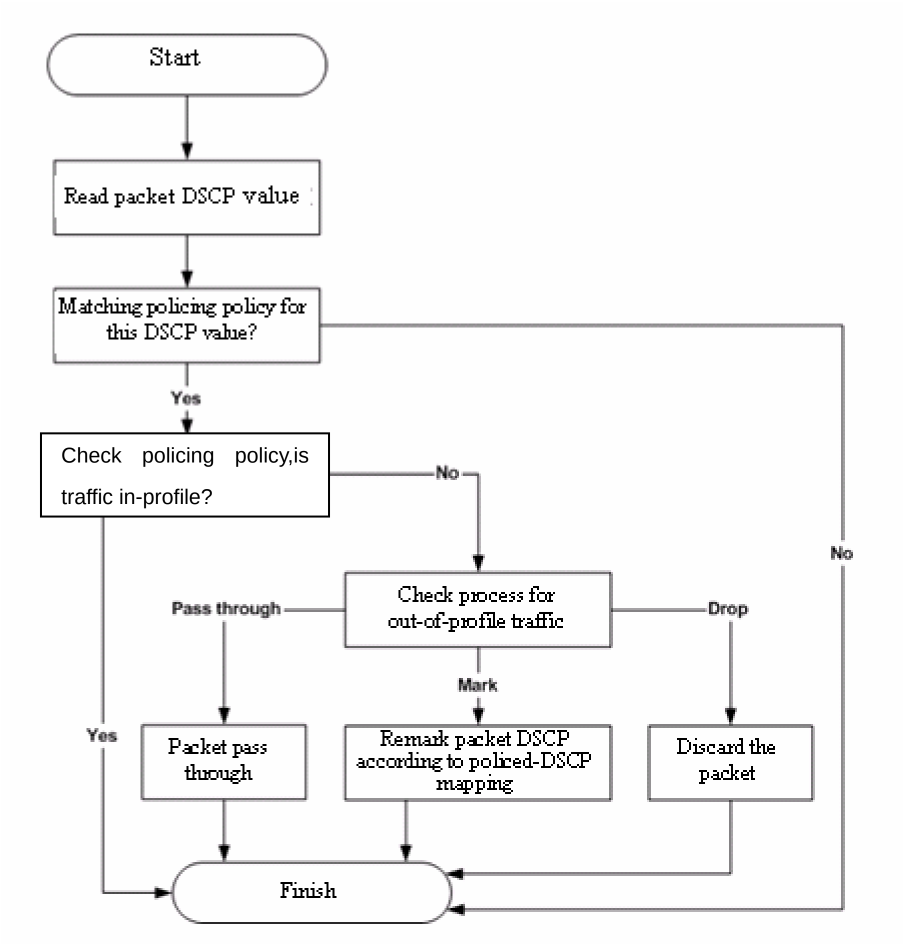

Start
Read packet DSCP value
Matching policing policy for this DSCP value?
Yes
Check policing policy,is traffic in-profile?
No
No
Check process for out-of-profile traffic
Pass through
Drop
Mark
Yes
Packet pass through
Remark packet DSCP according to policed-DSCP mapping
Discard the packet
Finish

Fig 1-5 Policing and Remarking process

Queuing and scheduling: Packets at the egress will re-map the internal DSCP value to CoS value, the queuing operation assigns packets to appropriate queues of priority according to the CoS value; while the scheduling operation performs packet forwarding according to the prioritized queue weight. The following flowchart describes the operations during queuing and scheduling.

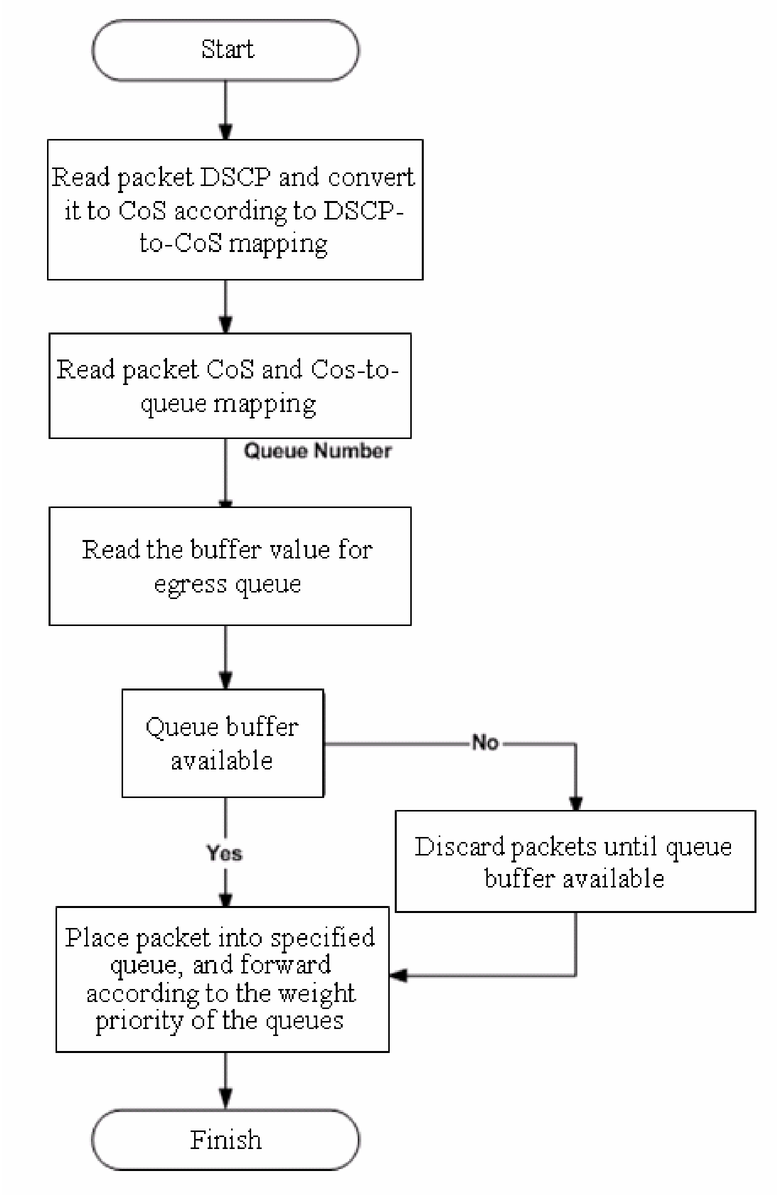

Start
Read packet DSCP and convert it to CoS according to DSCP-to-CoS mapping
Read packet CoS and Cos-to-queue mapping
Queue Number
Read the buffer value for egress queue
Queue buffer available
No
Discard packets until queue buffer available
Yes
Place packet into specified queue, and forward according to the weight priority of the queues
Finish

Fig 1-6Queuing and Scheduling process

1.1.2 QoS Configuration Task List

1. Enable QoS

   QoS can be enabled or disabled in Global Mode. QoS must be enabled first in Global Mode to configure the other QoS commands.

2. Configure class map.

   Set up a classification rule according to ACL, CoS, VLAN ID, IP Precedence or DSCP to classify the data stream. Different classes of data streams will be processed with different policies.

3. Configure a policy map.

After data steam classification, a policy map can be created to associate with the class map created earlier and enter class mode. Then different policies (such as bandwidth limit, priority degrading, assigning new DSCP value) can be applied to different data streams. You can also define a policy set that can be use in a policy map by several classes.

4. Apply QoS to the ports

   Configure the trust mode for ports or bind policies to ports. A policy will only take effect on a port when it is bound to that port.

5. Configure queue out method and weight

   Configure queue out to PQ or WRR, set the proportion of the 8 egress queues bandwidth and mapping from internal priority to egress queue.

6. Configure QoS mapping

   Configure the mapping from CoS to DSCP, DSCP to CoS, DSCP to DSCP mutation, IP precedence to DSCP, and policed DSCP.

7. Configure QoS apply to egress queue

1. Enable QoS

Command	Explanation
Global Mode	
mls qos **no mls qos**	Enable/disable QoS function.

2. Configure class map.

Command	Explanation
Global Mode	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	Create a class map and enter class map mode; the "**no class-map <*class-map-name*>**" command deletes the specified class map.

match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| ipv6 access-group <*acl-index-or-name*> | ipv6 dscp <*dscp-list*>| ipv6 flowlabel <*flowlabel-list*>| vlan <*vlan-list*>|cos<*cost-list*>}
no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan|cos }
	Set matching criterion (classify data stream by ACL, CoS, VLAN ID, IP Precedence or DSCP, etc) for the class map; the "**no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan|cos }**" command deletes specified matching criterion.

3. Configure a policy map.

Command	Explanation
Global Mode	
policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Create a policy map and enter policy map mode; the “**no policy-map <*policy-map-name*>**” command deletes the specified policy map.
class <*class-map-name*> **no class <*class-map-name*>**	After a policy map is created, it can be associated to a class. Different policy or new DSCP value can be applied to different data streams in class mode; the “**no class <*class-map-name*>**” command deletes the specified class.

set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>|ipv6 dscp <*new-dscp*> | ipv6 flowlabel <*new-flowlabel*>|cos<*new cos*>}
no set {ip dscp | ip precedence|ipv6 dscp | ipv6 flowlabel |cos<*new cos*>}
	Assign a new DSCP and IP precedence value for the classified traffic; the “**no set {ip dscp | ip precedence|ipv6 dscp | ipv6 flowlabel |cos<*new cos*>}**” command cancels the newly assigned.

policy <*bits_per_second*> <*normal_burst_bytes*> ({**conform-action** (**drop** | **set-dscp-transmit** <*dscp_value*> | **set-prec-transmit** <*ip_precedence_value*> | **transmit**) | **exceed-action** (**drop** | **policed-dscp-transmit** | **transmit**) } |) **no policy <*bits_per_second*> <*normal_burst_bytes*>** ({**conform-action** (**drop** | **set-dscp-transmit** <*dscp_value*> | **set-prec-transmit** <*ip_precedence_value*> | **transmit**) | **exceed-action** (**drop** | **policed-dscp-transmit** | **transmit**)} |) **policy <*bits_per_second*> <*normal_burst_bytes*>** (**pir <*peak_rate_bps*> |) <*maximum_burst_bytes*>** ({**conform-action** (**drop** | **set-dscp-transmit** <*dscp_value*> | **set-prec-transmit** <*ip_precedence_value*> |	The non-aggregation policer command supporting three colors. Determine whether the working mode of token bucket is singe rage single bucket, single rate single bucket, single rate dual bucket or dual rate dual bucket, by analyzing the parameters. The no command will delete the mode configuration.

transmit) **exceed-action** (**drop** | **policed-dscp-transmit** | **transmit**) | **violate-action** (**drop** | **policed-dscp-transmit | transmit)**} |) ***no*** **policy** ***<bits_per_second>*** ***<normal_burst_bytes>*** (**pir** ***<peak_rate_bps>*** **|)** ***<maximum_burst_bytes>*** ({**conform-action** (**drop | set-dscp-transmit** ***<dscp_value>*** **|** **set-prec-transmit** ***<ip_precedence_value>*** **|** **transmit**) **exceed-action** (**drop |** **policed-dscp-transmit | transmit**) **|** **violate-action** (**drop |** **policed-dscp-transmit | transmit)**} |)	
mls qos aggregate-policy ***<policer_name>*** ***<bits_per_second>*** ***<normal_burst_bytes>*** ({**conform-action** (**drop | set-dscp-transmit** ***<dscp_value>*** **| set-prec-transmit** ***<ip_precedence_value>*** **| transmit**) **|** **exceed-action** (**drop |** **policed-dscp-transmit | transmit**) } |) **mls qos aggregate-policy** ***<policer_name>*** ***<bits_per_second><normal_burst_bytes>***(**pir** ***<peak_rate_bps>*****|)*****<maximum_burst_bytes>*** ({**conform-action** (**drop** **|set-dscp-transmit** ***<dscp_value>*** **|set-prec-transmit** ***<ip_ precedence_value>*** **|transmit**) **exceed-action** (**drop|policed-dscp-transmit** **|transmit**)**|** **violate-action** (**dro** **|policed-dscp-transmit| transmit)**} |) **no mls qos aggregate-policy**	Analyze the working mode of the token bucket, whether it is single rate singe bucket, singe rate dual bucket or dual rate dual bucket. The no operation will delete the mode configuration.
policy aggregate ***<aggregate-policy-name>*** **no policy aggregate** ***<aggregate-policy-name>***	Apply a policy set to classified traffic; the "**no policy aggregate** ***<aggregate-policy-name>***" command deletes the specified policy set.

4. Apply QoS to ports or vlan interface

Command	Explanation
Interface Mode	
mls qos trust [cos [pass-through-dscp] [pass-through-cos]|dscp [pass-through-cos] [pass-through-dscp]|ip-precedence [pass-through-cos] [pass-through-dscp]|port priority <cos> [pass-through-cos] [pass-through-dscp]] **no mls qos trust**	Configure port trust; the "**no mls qos trust**" command disables the current trust status of the port.
mls qos cos {<*default-cos*> } **no mls qos cos**	Configure the default CoS value of the port; the "**no mls qos cos**" command restores the default setting.
service-policy input <*policy-map-name*> **no service-policy input <*policy-map-name*>**	Apply a policy map to the specified port or vlan interface; the "**no service-policy input <*policy-map-name*>**" command deletes the specified policy map applied to the port or vlan interface. Egress policy map is not supported yet.
mls qos dscp-mutation <*dscp-mutation-name*> **no mls qos dscp-mutation <*dscp-mutation-name*>**	Apply DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

5. Configure queue out method and weight

Command	Explanation
Interface Mode	
queue bandwidth<*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*>	Set the WRR weight for specified egress queue; the

no queue bandwidth	“**no queue bandwidth**” command restores the default setting.
queue mode strict **queue mode wrr**	the” **queue mode strict**” command configure queue out method to pq method; the “**queue mode wrr**” command restores the default WRR queue out method
Global Mode	
wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*> **no wrr-queue cos-map**	Set CoS value mapping to specified egress queue; the “**no wrr-queue cos-map**” command restores the default setting.

6. Configure QoS mapping

Command	Explanation
Global Mode	
mls qos map (cos-dscp <*dscp1...dscp8*> | dscp-cos <*dscp-list*> to <*cos*> | dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*> |ip-prec-dscp <*dscp1...dscp8*> | policed-dscp (normal-burst | max-burst) <*dscp-list*> to <*mark-down-dscp*>) **no mls qos map (cos-dscp | dscp-cos | dscp-mutation <*dscp-mutation-name*> | ip-prec-dscp | policed-dscp (normal-burst | max-burst))**	Support the configuration of all actions in dual rate dual bucket mode. Sets **class of service (CoS)-to-Differentiated Services Code Point (DSCP)** mapping, **DSCP to CoS** mapping, **DSCP to DSCP mutation** mapping, **IP precedence to DSCP** and **policed DSCP** mapping; the exceed-action and violate-action use different policied-dscp map tables. The no command restores the default mapping.

7. Configure QoS apply to egress queue

Command	Explanation

Interface Mode	
queue-bandwidth <*queue-id*> <*min_kbits_per_second*> <*max_kbits_per_second*> no queue-bandwidth <*queue-id*>	Configure the queue bandwidth pledge for export. The no command is to deleted the function.

1.2 Command for QoS

1.2.1.1 class

Command: class <*class-map-name*>

no class <class-map-name>

Function: Associates a class to a policy map and enters the policy class map mode; the "**no class <*class-map-name*>**" command deletes the specified class.

Parameters: < *class-map-name*> is the class map name used by the class.

Default: No policy class is configured by default.

Command mode: Policy map configuration Mode

Usage Guide: Before setting up a policy class, a policy map should be created and the policy map mode entered. In the policy class map mode,classification and policy configuration can be performed on packet traffic classified by class map.

Example: Entering a policy class mode.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#exit
```

1.2.1.2 match

Command:match {access-group <*acl-index-or-name*> | ip dscp <*dscp-list*>| ip precedence <*ip-precedence-list*>| ipv6 access-group <*acl-index-or-name*> | ipv6 dscp <*dscp-list*>| ipv6 flowlabel <*flowlabel-list*>| vlan <*vlan-list*>|cos<*cost-list*>}

no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan|cos }

Function: Configure the match standard of the class map; the "no" form of this command deletes the specified match standard..

Parameter: access-group <*acl-index-or-name*> match specified IP ACL or MAC ACL, the parameters are the number or name of the ACL;**ip dscp <*dscp-list*>** and **ipv6 dscp <*dscp-list*>** match specified DSCP value, the parameter is a list of DSCP consisting of maximum 8 DSCP values;**ip precedence <*ip-precedence-list*>** match specified IP Precedence, the parameter is a IP Precedence list consisting of maximum 8 IP Precedence values with a valid range of 0～

7;**ipv6 access-group <*acl-index-or-name*>** match specified IPv6 ACL,the parameter is the number or name of the IPv6 ACL;**ipv6 flowlabel <*flowlabel-list*>** match specified IPv6 flow label, the parameter is IPv6 flow label value;**vlan <*vlan-list*>** match specified VLAN ID, the parameter is a VLAN ID list consisting of maximum 8 VLAN IDs.**<*cost-list*>** match specified cos value, the patameter is a COS list consisting of maximum 8 Cos.

Default: No match standard by default

Command Mode: Class-map Mode

Usage Guide: Only one match standard can be configured in a class map. When configuring match the ACL, only the permit rule is available in the ACL except for PBR.

Example: Create a class-map named c1, and configure the class rule of this class-map to match packets with IP Precedence of 0.1.

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match ip precedence 0 1
Switch(Config-ClassMap-c1)#exit
```

1.2.1.3 set

Command:set {ip dscp <*new-dscp*> | ip precedence <*new-precedence*>|ipv6 dscp <*new-dscp*> | ipv6 flowlabel <*new-flowlabel*>|cos<*new cos*>}

no set {ip dscp | ip precedence|ipv6 dscp | ipv6 flowlabel |cos<*new cos*>}

Function: Assign a new DSCP, IP Precedence, IPv6 DSCP or IPv6 FL for the classified traffic; the "no" form of this command delete assigning the new values

Parameter:<*new-dscp*>new DSCP value;**<*new-precedence*>**new IP IPv4 Precedence;**<*new-flowlabel*>** new IPv6 FL value **<*new cos*>}** new COS value

Default: Not assigning by default

Command Mode: Policy Class-map Mode

Usage Guide: Only the classified traffic which matches the matching standard will be assigned with the new values.

Example: Set the IP Precedence of the packets matching the c1 class rule to 3.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

1.2.1.4 class-map

Command:class-map <*class-map-name*>

no class-map <*class-map-name*>

Function: Creates a class map and enters class map mode; the "**no class-map**

<class-map-name>" command deletes the specified class map.

Parameters: <*class-map-name*> is the class map name**.**

Default: No class map is configured by default.

Command mode: Global Mode

Example: Creating and then deleting a class map named "c1".

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#exit
Switch(config)#no class-map c1
```

1.2.1.5 mls qos

Command:mls qos

no mls qos

Function: Enables QoS in Global Mode; the "**no mls qos**" command disables the global QoS.

Command mode: Global Mode

Default: QoS is disabled by default.

Usage Guide: QoS provides 8 queues to handle traffics of 8 priorities. T The rule is taking effect by default when startup, message will rewrite cos field according to cos-dscp-cos, dscp-mutation rewrite dscp value according to cos-dscp. Ingress cos value is the port default cos.

Example: Enable and then disabling the QoS function.

```
Switch(config)#mls qos
Switch(config)#no mls qos
```

1.2.1.6 mls qos cos

Command:mls qos cos {<*default-cos*> }

no mls qos cos

Function: Configures the default CoS value of the port; the "**no mls qos cos**" command restores the default setting.

Parameters: < *default-cos*> is the default CoS value for the port, the valid range is 0 to 7.

Default: The default CoS value is 0.

Command mode: Interface Mode

Usage Guide: Configure the default CoS value for switch port. The message ingress cos from this port are default value whether the message have tag. If the message have no tag, the message cos value for tag is enactmented.

Example: Setting the default CoS value of Ethernet port 1/1 to 5, i.e., packets coming in through this port will be assigned a default CoS value of 5 if no CoS value present.

```
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#mls qos cos 5
```

1.2.1.7 mls qos aggregate-policy

Command: Single Bucket Mode:

mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> ({conform-action (drop | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | transmit) | exceed-action (drop | policed-dscp-transmit | transmit) })

no mls qos aggregate-policy

Dual Bucket Mode:

mls qos aggregate-policy <policer_name> <bits_per_second> <normal_burst_bytes> (pir <peak_rate_bps> |) <maximum_burst_bytes> ({conform-action (drop | set-dscp-transmit <dscp_value> | set-prec-transmit <ip_precedence_value> | transmit) exceed-action (drop | policed-dscp-transmit | transmit) | violate-action (drop | policed-dscp-transmit | transmit)})

no mls qos aggregate-policy

Function: Analyze the working mode of the token bucket, whether it is single rate singe bucket, singe rate dual bucket or dual rate dual bucket. The no operation will delete the mode configuration.

Parameters: policer_name：the name of aggregation policer;

bits_per_second：the committed information rate - CIR , in Kbps, ranging from 1 to 10000000;

normal_burst_bytes：the committed burst size – CBS, in kb, ranging from 1 to 1000000. When the configured CBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt;

pir peak_rate_bps：the peak information rate, in kbps, ranging from 1to 1～10000000. Without configuring PIR, the Police works in the single rate dual bucket mode; otherwise in the dual rate dual bucket mode. Notice: this configuration only exist in the dual bucket mode. Notice: this configuration only exists in dual bucket mode;

maximum_burst_bytes：the peak burst size, in kb, ranging from 1to 1～10000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode;

conform-action：the actions to take when the CIR is not exceeded, which means the messages are green, including drop;

set-dscp-transmit：change dscp (ranging from 0 to 63), set-prec-transmit: change TOS (ranging from 0 to 1), transmit: messages will pass without any action;

exceed-action：the actions to take when the CIR is exceeded but PIR isn't, which means the messages are yellow, including drop, policed-dscp-transmit: mark down the packets DSCP value, transmit: messages will pass without any action;

violate-action：the actions to take when the PIR is exceeded, which means the messages are red, including drop, policed-dscp-transmit: mark down the packets DSCP value, transmit: messages will pass without any action. Notice: this action only exists in dual bucket mode.

Default: No aggregation Policer is defined by default; the default action of conform-action is “transmit”, while that of exceed-action and violate-action both is drop.

Command mode: Global Mode

Usage Guide: The CLI can support both singe bucket and dual bucket configuration, and determine which one to select by checking whether violate-action is configured. When configuring with CLI, after configuring CBS, if the action is directly configured, the mode is single rate single bucket; if only PBS is configured, the mode is single rate dual bucket; if PIR and PBS are configured, the mode is dual rate dual bucket.

Example: Set the single bucket mode, CIR is 1000, CBS is 1000. The action to take is drop, when the CIR is not exceeded, which means the messages are green; the action is policed-dscp-transmit (change the DSCP value and then transmit the messages) when the CIR is exceeded but PIR isn’t, which means the messages are yellow.

Switch(config)#mls qos aggregate-policy color 1000 1000 conform-action drop exceed-action policed-dscp-transmit

1.2.1.8 mls qos trust

Command: mls qos trust {cos [pass-through-cos] [pass-through-dscp]|dscp [pass-through-cos] [pass-through-dscp]| ip-precedence [pass-through-cos] [pass-through-dscp] |port priority <*cos*> [pass-through-cos] [pass-through-dscp]}

Function: Configures port trust; the “**no mls qos trust**” command disables the current trust status of the port.

Parameters: trust cos mode: can setting the message cos field based cos-dscp-cos, setting the message dscp value based cos-dscp, dscp-mutation. If the port have configured dscp-mutation, the pass-through-dscp command can not be used.

trust dscp mode: can setting the message cos field based dscp-cos, setting the message dscp value based dscp-mutation. If the port have configured dscp-mutation, the pass-through-dscp command can not be used.

trust ip-precedence mode: can setting the message cos field based ip-precedence-dscp-cos, setting the message dscp value based ip-precedence-dscp，dscp-mutation. If the port have configured dscp-mutation, the pass-through-dscp command can not be used.

trust port mode: can setting the message cos field based cos-dscp-cos, setting the message dscp value based cos-dscp，dscp-mutation. If the port have configured dscp-mutation, the pass-through-dscp command can not be used.

Default: No trust

Command mode: Interface Mode

Usage Guide: For packets with both CoS value and DSCP value,keyword **pass-through** should be used to protect the value if the value should not be changed after classification.

Example: Configuring Ethernet port 1/1 to trust CoS value, i.e., classifying the packets according to CoS value, DSCP value should not be changed.

Switch(config)#interface ethernet 1/1

Switch(Config-If-Ethernet1/1)#mls qos trust cos pass-through-dscp

1.2.1.9 mls qos dscp-mutation

Command:mls qos dscp-mutation <*dscp-mutation-name*>

no mls qos dscp-mutation <*dscp-mutation-name*>

Function: Applies DSCP mutation mapping to the port; the "**no mls qos dscp-mutation <*dscp-mutation-name*>**" command restores the DSCP mutation mapping default.

Parameters: <*dscp-mutation-name*> is the name of DSCP mutation mapping.

Default: There is no policy by default.

Command mode: Interface Mode

Usage Guide: For configuration of DSCP mutation mapping on the port to take effect, the port can configure no trust status or configure any trust status, but can not be used with pass-through-dscp command in trust status. DSCP mutation mapping is good for this port.

Example: Configuring Ethernet port 1/1 to trust DSCP, using DSCP mutation mapping of mu1.

Switch(config)#interface ethernet 1/1

Switch(Config-If-Ethernet1/1)#mls qos trust dscp pass-through-cos

Switch(Config-If-Ethernet1/1)#mls qos dscp-mutation mu1

1.2.1.10 mls qos map

Command: mls qos map (cos-dscp <dscp1...dscp8> | dscp-cos <dscp-list> to <cos> | dscp-mutation <dscp-mutation-name> <in-dscp> to <out-dscp> |ip-prec-dscp <dscp1...dscp8> | policed-dscp (normal-burst | max-burst) <dscp-list> to <mark-down-dscp>)

no mls qos map (cos-dscp | dscp-cos | dscp-mutation <dscp-mutation-name> | ip-prec-dscp | policed-dscp (normal-burst | max-burst))

Function: Support the configuration of all actions in dual rate dual bucket mode. Sets **class of service (CoS)-to-Differentiated Services Code Point (DSCP)** mapping, **DSCP to CoS** mapping, **DSCP to DSCP mutation** mapping, **IP precedence to DSCP** and **policed DSCP** mapping; the exceed-action and violate-action use different policied-dscp map tables. The no command restores the default mapping.

Parameters: cos-dscp <*dscp1...dscp8*> defines the mapping from CoS value to DSCP-inside, **<*dscp1...dscp8*>** are the 8 DSCP-inside value corresponding to the 0 to 7 CoS value, each DSCP-inside value is delimited with space, ranging from 0 to 63; **dscp-cos <*dscp-list*> to <*cos*>** defines the mapping from DSCP-inside to CoS value, **<*dscp-list*>** is a list of DSCP value consisting of up to 8 DSCP-inside values, **<*cos*>** are the CoS values corresponding to the DSCP values in the list; **dscp-mutation <*dscp-mutation-name*> <*in-dscp*> to <*out-dscp*>** defines the mapping from DSCP to DSCP mutation, **<*dscp-mutation-name*>** is the name for mutation mapping, **<*in-dscp*>** stand for incoming DSCP-inside values, up to 8 values are supported, each DSCP-inside value is delimited with space, ranging from 0 to 63, **<*out-dscp*>** is the sole outgoing DSCP value, the 8 values defined in incoming DSCP will be converted to outgoing DSCP values; **ip-prec-dscp <*dscp1...dscp8*>** defines the conversion from IP precedence to DSCP-inside value, **<*dscp1...dscp8*>** are 8 DSCP-inside values corresponding to IP precedence 0 to 7, each DSCP value is delimited with space, ranging from 0 to 63; **policed-dscp <*dscp-list*> to <*mark-down-dscp*>** defines DSCP **mark down** mapping, where **<*dscp-list*>** is a list of DSCP values containing up to 8 DSCP values, **<*mark-down-dscp*>** are DSCP value after **mark down**.

Default: Default mapping values are:

Default CoS-to-DSCP Map

CoS Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Default DSCP-to-CoS Map

DSCP Value	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS Value	0	1	2	3	4	5	6	7

Default IP-Precedence-to-DSCP Map

IP Precedence Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

dscp-mutation and policed-dscp are not configured by default

Command mode: Global Mode

Usage Guide: The dscp which in cos-dscp, dscp-cos, ip-prec-dscp, dscp-mutation fingers dscp-inside value. Because of the dscp-inside value have 64 and that the chip priority-inside only 8, the dscp-cos mapping need 8 continuum dscp-inside mapping to the same cos, in other words, dscp 0-7 mapping the same cos value.

Example: 1. Setting the ***CoS-to-DSCP*** mapping value to the default 0 8 16 24 32 40 48 56 to 0 1 2 3 4 5 6 7.

Switch(config)#mls qos map cos-dscp 0 1 2 3 4 5 6 7

2. Mapping DSCP 1, 2 to COS 7.

Switch(config)#mls qos map dscp-cos 1 2 to 7

1.2.1.11 policy

Command: Single Bucket Mode:

policy <*bits_per_second*> <*normal_burst_bytes*> ({**conform-action** (**drop** | **set-dscp-transmit <*dscp_value*> | set-prec-transmit <*ip_precedence_value*> | transmit**) |

exceed-action (**drop** | **policed-dscp-transmit** | **transmit**) } |)
no policy ***<bits_per_second>*** ***<normal_burst_bytes>*** ({**conform-action** (**drop** | **set-dscp-transmit** ***<dscp_value>*** | **set-prec-transmit** ***<ip_precedence_value>*** | **transmit**) | **exceed-action** (**drop** | **policed-dscp-transmit** | **transmit**)})

Dual Bucket Mode:

policy ***<bits_per_second>*** ***<normal_burst_bytes>*** (**pir** ***<peak_rate_bps>*** **|)** ***<maximum_burst_bytes>*** ({**conform-action** (**drop** | **set-dscp-transmit** ***<dscp_value>*** | **set-prec-transmit** ***<ip_precedence_value>*** | **transmit**) **exceed-action** (**drop** | **policed-dscp-transmit** | **transmit**) | **violate-action** (**drop** | **policed-dscp-transmit** | **transmit)**})
no policy ***<bits_per_second>*** ***<normal_burst_bytes>*** (**pir** ***<peak_rate_bps>*** **|)** ***<maximum_burst_bytes>*** ({**conform-action** (**drop** | **set-dscp-transmit** ***<dscp_value>*** | **set-prec-transmit** ***<ip_precedence_value>*** | **transmit**) **exceed-action** (**drop** | **policed-dscp-transmit** | **transmit**) | **violate-action** (**drop** | **policed-dscp-transmit** | **transmit)**})

Function: The non-aggregation policer command supporting three colors. Determine whether the working mode of token bucket is singe rage single bucket, single rate single bucket, single rate dual bucket or dual rate dual bucket, by analyzing the parameters. The no command will delete the mode configuration.

Parameters: bits_per_second： the committed information rate - CIR , in Kbps, ranging from 1 to 10000000.

normal_burst_bytes：the committed burst size – CBS, in kb, ranging from 1 to 1000000. When the configured CBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt.

maximum_burst_bytes：the peak burst size, in kb, ranging from 1to 1～10000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode.

pir peak_rate_bps：the peak burst size, in kb, ranging from 1to 1～10000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode.

conform-action：the actions to take when the CIR is not exceeded, which means the messages are green, including drop, **set-dscp-transmit:** change dscp (ranging from 0 to 63), set-prec-transmit: change TOS (ranging from 0 to 1), transmit: messages will pass without any action.

exceed-action：the actions to take when the CIR is exceeded but PIR isn’t, which means the messages are yellow, including drop, policed-dscp-transmit: mark down the packets DSCP value, transmit: messages will pass without any action.

violate-action：the actions to take when the PIR is exceeded, which means the messages are red, including drop, policed-dscp-transmit: mark down the packets DSCP value, transmit: messages will pass without any action. Notice: this action only exists in dual bucket mode.

Default: No aggregation Policer is defined by default; the default action of conform-action is "transmit", while that of exceed-action and violate-action both is drop. "show running-config" won't display the default configurations.

Command mode: Policy class map configuration Mode

Usage Guide: The CLI can support both singe bucket and dual bucket configuration, and determine which one to select by checking whether violate-action is configured. When configuring with CLI, after configuring CBS, if the action is directly configured, the mode is single rate single bucket; if only PBS is configured, the mode is single rate dual bucket; if PIR and PBS are configured, the mode is dual rate dual bucket.

Example: In the policy class table configuration mode, set the CIR as 1000, CBS as 2000 and the action when CIR is not exceeded as transmitting the messages after changing DSCP to 23, and the action triggered by exceeding CIR as transmit without changing the messages.

```
Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
Switch(config-policymap-1-class-cm)#policy 1000 2000 conform-action set-dscp-transmit 23 exceed-action transmit
```

1.2.1.12 policy aggregate

Command: policy aggregate <*aggregate-policy-name*>

no policy aggregate <*aggregate-policy-name*>

Function: Police Map reference aggregate policy, applies a policy set to classified traffic; the "**no policy aggregate <*aggregate-policy-name*>**" command deletes the specified policy set.

Parameters: <*aggregate-policy-name*> is the policy set name.

Default: No policy set is configured by default.

Command mode: Policy class map configuration Mode

Usage Guide: The same policy set can be referred to by different policy class maps.

Example: Create class-map, the match rule is "the cos value is 0"; policy-map is 1, enter the policy map mode, set the Policy and choose the color policy for the current list.

```
Switch(config)#class-map cm
Switch(config-classmap-cm)#match cos 0
Switch(config-classmap-cm)#exit
Switch(config)#policy-map 1
Switch(config-policymap-1)#class cm
```

Switch(config-policymap-1-class-cm)#policy aggregate color

1.2.1.13 policy-map

Command:policy-map <*policy-map-name*>

no policy-map <*policy-map-name*>

Function: Creates a policy map and enters the policy map mode; the "**no policy-map <*policy-map-name*>**" command deletes the specified policy map.

Parameters: < *policy-map-name*> is the policy map name.

Default: No policy map is configured by default.

Command mode: Global Mode

Usage Guide: QoS classification matching and marking operations can be done in the policy map configuration mode.

Example: Creating and deleting a policy map named "p1".

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#exit
Switch(config)#no policy-map p1
```

1.2.1.14 queue mode

Command: queue mode {strict|wrr}

Function: Configure the queue out mode.

Parameter: strict configure queue out method to strict priority-queue method; wrr restores the default wrr queue out method.

Default: wrr out queue mode

Command mode: Interface Mode

Usage Guide: When priority-queue queue out mode is used, packets are no longer sent with WRR weighted algorithm, but send packets queue after queue.

Example: Set the queue out mode to strict priority-queue.

```
Switch(Config-If-Ethernet )#queue mode strict
```

1.2.1.15 queue-bandwidth

Command: queue-bandwidth <*queue-id*> <*min_kbits_per_second*> <*max_kbits_per_second*>

no queue-bandwidth <*queue-id*>

Function: Configure the queue bandwidth pledge for export.

Parameter: <*queue-id*> is the queen ID to pledge, the queue count is difference toward different chip, the range is difference too, the normal instance is 8 queue, range from 1 to 8. **<*min_kbits_per_second*>** is the min-bandwidth, range from 0 to 128000, when input0, it means that the min-bandwidth function failure. ***<max_kbits_per_second>*** is the max-bandwidth, range from 0 to 128000, when input 0, it means that the max-bandwidth function failure. But the min-bandwidth and max-bandwidth are not allow to input 0 at the same time, and the min-bandwidth must not larger than max-bandwidth.

Default: The queue bandwidth have no pledge by default.

Command mode: Interface Mode

Usage Guide: The min-bandwidth and max-bandwidth for queue can be configured alone, and can be configured at only one queue. For example: if want to limit the bandwidth to 128kbps for export Ethernet1/2 queue 1, it just need to configure that queue-bandwidth 1 0 128.

The queue bandwidth pledge for export is correlation to queue mode, for example: one port is strict priority-queue, the tiptop priority is queue 1 now, it will pri-content this queue flux when congestion. But if user configure the queue bandwidth pledge for this port"s low-priority queue, it can obligate bandwidth for this queue, the low-priority queue's min-bandwidth will be content first, then the residue bandwidth be allotted according to PQ.

Example: Configure the min-bandwidth is 64kbps and the max-bandwidth is 128kbps for ethernet1/2 queue1.

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#queue-bandwidth 1 64 128
```

1.2.1.16 service-policy

Command: service-policy input <*policy-map-name*>

no service-policy input <*policy-map-name*>

Function: Applies a policy map to the specified port or vlan interface; the "**no service-policy input <*policy-map-name*>**" command deletes the specified policy map applied to the port or vlan interface.

Parameters: input <*policy-map-name*> applies the specified policy map to the ingress of switch port or vlan interface.

Default: No policy map is bound to ports and vlan interface by default.

Command mode: Interface Mode(switch port or vlan interface)

Usage Guide: Configuring port trust status and applying policy map on the port are two conflicting operations; the later configuration will override the earlier configuration. Only one policy map can be applied to each direction of each port or vlan interface. Egress policy map is not supported yet.

Example: Bind policy p1 to ingress Ethernet port 1/1.

```
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)# service-policy input p1
```

Bind policy p1 to ingress interface vlan 1.

```
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#service-policy input p1
```

1.2.1.17 queue bandwidth

Command: queue bandwidth<*weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*>

no queue bandwidth

Function: Sets the WRR weight for specified egress queue; the "**no queue bandwidth**" command restores the default setting.

Parameters: *<weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8>* are WRR weights, ranging from 0 to 15.

Default: The default values of weight1 to weight8 are 1 through 8. .

Command mode: Interface Mode

Usage Guide: The absolute value of WRR is meaningless. WRR allocates bandwidth by using eight weight values' proportion. If a weight is 0, then the queue has the highest priority; when the weights of multiple queues are set to 0, then the queue of higher order has the higher priority.

Example: Setting the bandwidth weight proportion of the eight queue out to be 1:1:2:2:4:4:8:8.

```
Switch(Config-If-Ethernet1/1)#queue bandwidth1 1 2 2 4 4 8 8
```

1.2.1.18 wrr-queue cos-map

Command: wrr-queue cos-map <*queue-id*> <*cos1 ... cos8*>

no wrr-queue cos-map

Function: Sets the CoS value mapping to the specified queue out; the "**no wrr-queue cos-map**" command restores the default setting.

Parameters: *<queue-id>* is the ID of queue out, ranging from 1 to 8; ***<cos1 ... cos8>*** are CoS values mapping to the queue out, ranging from 0 -7, up to 8 values are supported.

Default:

Default CoS-to-Egress-Queue Map when QoS is Enabled

CoS Value	0	1	2	3	4	5	6	7
Queue Selected	1	2	3	4	5	6	7	8

Command mode: Global Mode

Usage Guide:

Example: Mapping packets with CoS value 2 and 3 to egress queue 1.

```
Switch(config)#wrr-queue cos-map 1 2 3
```

1.2.2 QoS Example

Scenario 1:

Enable QoS function, change the queue out weight of port ethernet 1/1 to 1:1:2:2:4:4:8:8, and set the port in trust QoS mode without changing DSCP value, and set the default QoS value of the port to 5.

The configuration steps are listed below:

```
Switch#config
Switch(config)#mls qos
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#queue bandwidth1 1 2 2 4 4 8 8
Switch(Config-If-Ethernet1/1)#mls qos trust cos pass-through-dscp
Switch(Config-If-Ethernet1/1)#mls qos cos 5
```

Configuration result:

When QoS enabled in Global Mode, the egress queue bandwidth proportion of port ethernet 1/1 is 1:1:2:2:4:4:8:8. When packets have CoS value coming in through port ethernet 1/1, it will be map to the queue out according to the CoS value, CoS value 0 to 7 correspond to queue out 1, 2, 3, 4, 5, 6, 7, 8, respectively. If the incoming packet has no CoS value, it is default to 5 and will be put in queue 6. All passing packets would not have their DSCP values changed.

Scenario 2:

In port ethernet 1/2, set the bandwidth for packets from segment 192.168.1.0 to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting will be dropped.

The configuration steps are listed below:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#policy 10000 4000 exceed-action drop
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#service-policy input p1
```

Configuration result:

An ACL name 1 is set to matching segment 192.168.1.0. Enable QoS globally, create a class map named c1, matching ACL1 in class map; create another policy map named p1 and refer to c1 in p1, set appropriate policies to limit bandwidth and burst value. Apply this policy map on port ethernet 1/2. After the above settings done, bandwidth for packets from segment 192.168.1.0 through port ethernet 1/2 is set to 10 Mb/s, with a burst value of 4 MB, all packets exceed this bandwidth setting in that segment will be dropped.

Scenario 3:

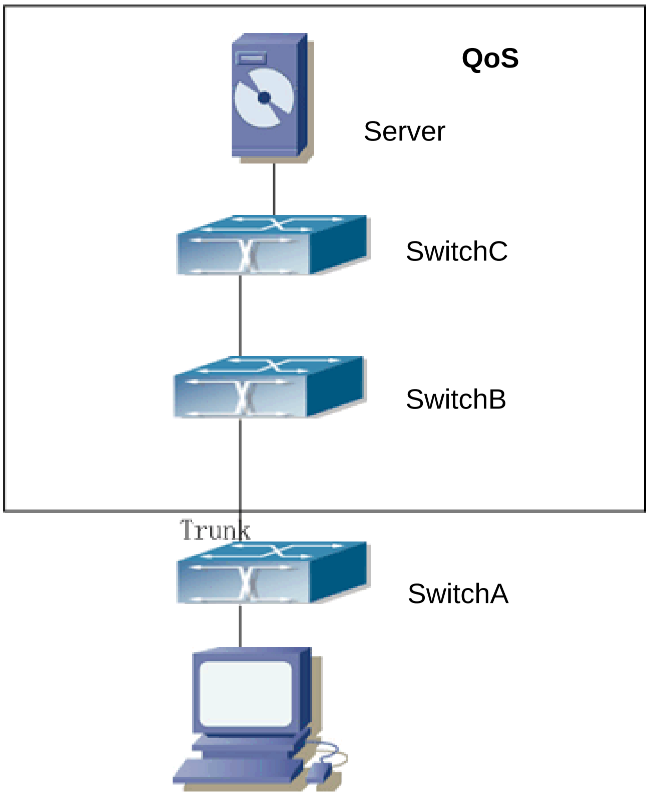


Fig 1-7 Typical QoS topology

As shown in the figure, inside the block is a QoS domain, switchA classifies different traffics and assigns different IP precedences. For example, set IP precedence for packets from segment 192.168.1.0 to 5 on port ethernet 1/1. The port connecting to switchB is a trunk port. In SwitchB, set port ethernet 1/1 that connecting to swtichA to trust IP precedence. Thus inside the QoS domain, packets of different priorities will go to different queues and get different bandwidth.

The configuration steps are listed below:

QoS configuration in SwitchA:

```
Switch#config
Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 5
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#service-policy input p1
```

QoS configuration in SwitchB:

```
Switch#config
Switch(config)#mls qos
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#mls qos trust ip-precedence pass-through-cos
```

1.2.3 QoS Troubleshooting Help

- ☞ QoS is disabled on switch ports by default, 8 sending queues are set by default, queue1 forwards normal packets, other queues are used for some important control packets (such as BPDU).
- ☞ When QoS is enabled in Global Mode,. QoS is enabled on all ports with 8 traffic queues. The default CoS value of the port is 0; the port is in not Trusted state by default; the default queue weight values are 1, 2, 3, 4, 5, 6, 7, 8 in order, all QoS Map is using the default value.
- ☞ CoS value 7 maps to queue 8 that has the highest priority and usually reserved for certain protocol packets. It is not recommended for the user to change the mapping between CoS 7 to Queue 8, or set the default port CoS value to 7.
- ☞ Policy map can only be bound to ingress direction, egress is not supported yet.
- ☞ If the policy is too complex to be configured due to hardware resource limit, error massages will be provided.

1.2.3.1 Monitor And Debug Command

1.2.3.1.1 show class-map

Command: show class-map [<*class-map-name*>]

Function: Displays class map of QoS.

Parameters: < *class-map-name*> is the class map name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Displays all configured class-map or specified class-map information.

Example:

```
Switch#show class-map
Class map name:c1, used by 1 times
  match acl name:1
```

Displayed information	Explanation
Class map name:c1	Name of the Class map
used by 1 times	Used times
match acl name:1	Classifying rule for the class map.

1.2.3.1.2 show policy-map

Command: show policy-map [<*policy-map-name*>]

Function: Displays policy map of QoS.

Parameters: < *policy-map-name*> is the policy map name.

Default: N/A.

Command mode: Admin Mode

Usage Guide: Displays all configured policy-map or specified policy-map information.

Example:

Example: Displays policy map of QoS.

```
Switch#show policy -map
Policy Map p1
  Class Map name: c1
    police 16000000 2000 conform-action drop exceed-action transmit
```

Displayed information	Explanation
Policy Map p1	Name of policy map
Class map name:c1	Name of the class map referred to
police 16000000 2000 conform-action drop exceed-action transmit	Policy implemented

1.2.3.1.3 show mls qos aggregate-policy

Command: show mls qos aggregate-policy [<*aggregate-policy-name*>]

Function: Displays policy set configuration information for QoS.

Parameters: <*aggregate-policy-name*> is the policy set name.

Default: N/A.

Command mode: Admin Mode

Usage Guide:

Example:

```
Switch(config)#show mls qos aggregate-policy a2
aggregate policy a2 10 10 10 conform-action set-dscp-transmit 7
      Not used by any policy map
```

Displayed information	Explanation
aggregate policy a2 10 10 10 conform-action set-dscp-transmit 7	Configuration for this policy set.
Not used by any policy map	Time that the policy set is being referred to

1.2.3.1.4 show mls qos interface

Command: show mls qos interface [<*interface-id*>] [buffers | policy | queuing | statistics]

Function: Displays QoS configuration information on a port.

Parameters: <***interface-id***> is the port ID; **buffers** is the queue buffer setting on the port; **policy** is the policy setting on the port; **queuing** is the queue setting for the port; **statistics** is the number of packets allowed to pass for in-profile and out-of-profile traffic according to the policy bound to the port.

Default: N/A.

Command mode: Admin Mode

Usage Guide: In single rate single bucket mode, the messages can only red or green when passing police. In the print information, in-profile means green and out-profile means red. In dual bucket mode, there are three colors of messages. But the counter can only count two kinds of messages, the red and yellow ones will both be treated as out-profile. Only when configuring ingress policies, there is statistic information.

Example:

```
Switch #show mls qos interface ethernet 1/2
Ethernet1/2
default cos:0
DSCP Mutation Map: Default DSCP Mutation Map
   Attached policy map for Ingress: p1
```

Displayed information	Explanation
Ethernet1/2	Port name
default cos:0	Default CoS value of the port.
DSCP Mutation Map: Default DSCP Mutation Map	Port DSCP map name
Attached policy map for Ingress: p1	Policy name bound to port.

```
Switch# show mls qos interface buffers ethernet 1/2
```

```
Ethernet 1/2
        packet   number of 8 queue:
        0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200
```

Displayed information	Explanation
packet number of 8 queue: 0x200 0x200 0x200 0x200 0x200 0x200 0x200 0x200	Available packet number for all 8 queues out on the port, this is a fixed setting that cannot be changed.

```
Switch# show mls qos interface queuing ethernet 1/2
Cos-queue map:
         Cos     0      1      2      3      4      5      6      7
         Queue 1        2      3      4      5      6      7      8

Queue and weight type:
         Port           q1     q2     q3     q4     q5     q6     q7     q8     QType
         Ethernet1/2    1      2      3      4      5      6      7      8      WRR
```

Displayed information	Explanation
Cos-queue map:	CoS value to queue mapping.
Queue and weight type:	Queue to weight mapping.
QType	WRR or PQ queue out method

```
Switch# show mls qos interface policy ethernet 1/2
Ethernet 1/2
    Attached policy-map for Ingress: p1
```

Displayed information	Explanation
Ethernet1/2	Port name
Attached policy-map for Ingress: p1	Policy map bound to the port.

```
Switch# show mls qos interface statistics ethernet 1/2
Device: Ethernet 1/2
     Classmap      classified      in-profile      out-profile (in packets)
           c1             0                  0                  0
```

Displayed information	Explanation
Ethernet1/2	Port name
ClassMap	Name of the Class map
Classified	Total data packets match this class map.

in-profile	Total in-profile data packets match this class map.
out-profile	Total out-profile data packets match this class map.

1.2.3.1.5 show mls qos maps policed-dscp

Command: show mls qos maps policed-dscp [normal-burst|max-burst]

Function: Display the configuration of policed-dscp map.

Parameters: normal-burst map for the yellow messages. **max-burst** map for the red messages. No parameter means to print both maps

Default: N/A.

Command mode: Admin and Config Mode.

Usage Guide: Display the map configuration information of QoS.

Example: Display the policed-dscp the map configuration information, here are some examples.

```
Switch(config)#show mls qos maps policed-dscp
Normal Burst Policed-dscp map:
      d1 : d2 0   1   2   3   4   5   6   7   8   9
      0:        0   1   2   3   4   5   6   7   8   9
      1:       10 11 12 13 14 15 16 17 18 19
      2:       20 21 22 23 24 25 26 27 28 29
      3:       30 31 32 33 34 35 36 37 38 39
      4:       40 41 42 43 44 45 46 47 48 49
      5:       50 51 52 53 54 55 56 57 58 59
      6:       60 61 62 63

Maximum Burst Policed-dscp map:
      d1 : d2 0   1   2   3   4   5   6   7   8   9
      0:        0   7   7   7   7   7   6   7   8   9
      1:       10 11 12 13 14 15 16 17 18 19
      2:       20 21 22 23 24 25 26 27 28 29
      3:       30 31 32 33 34 35 36 37 38 39
      4:       40 41 42 43 44 45 46 47 48 49
      5:       50 51 52 53 54 55 56 57 58 59
      6:       60 61 62 63
```

1.2.3.1.6 show mls-qos

Command: show mls-qos

Function: Displays global configuration information for QoS.

Parameters: N/A.

Default: N/A.

Command mode: Admin Mode

Usage Guide: This command indicates whether QoS is enabled or not.

Example:

```
Switch #show mls-qos
Qos is enabled!
```

Displayed information	Explanation
Qos is enabled!	QoS is enabled.

1.3 PBR Configuration

1.3.1 Introduction to PBR

PBR（Policy-Based Routing）is a method which determines the next-hop of the data packets by policy messages such as source address, destination address, IP priority, TOS value, IP protocol, source port No, destination port No, etc.

1.3.2 PBR configuration

The PBR configuration task list is as follows:

Initiate PBR function

Enable or disable PBR function automatically when turn on or turn off the QoS function at global mode.

Config classmap

Establish a class rule and apply different policies on different kinds of data streams thereafter.

Config policymap

A policymap can be established after the data streams are classified. Assign each stream to previously created classmap and then enter the policy classmap mode. In this way different data streams can now be assigned to different next-hop IP address and apply the policy to the port.

Apply policymap

A policy will not be valid until it is bonded to a specified port.

1.3.3 PBR examples

On port ethernet 1/1, apply policy-based routing on packages from 192.168.1.0/24 segment, and set the next-hop as 218.31.1.119, meanwhile the local network IP of this network ranges within 192.168.0.0/16. To assure normal communication in local network, messages from 192.168.1.0/24 to local IP 192.168.0.0/16 are not applied with policy routing.

Configuration procedure is as follows:

```
Switch#config
```

```
Switch(config)#access-list ip extended a1
Switch(Config-IP-Ext-Nacl-a1)#permit ip 192.168.1.0 0.0.0.255 any-destination
Switch(Config-IP-Ext-Nacl-a1)#deny ip 192.168.1.0 0.0.0.255 192.168.0.0 0.0.255.255
Switch(Config-IP-Ext-Nacl-a1)#exit
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group a1
Switch(Config-ClassMap-c1)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip nexthop 218.31.1.119
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet
Switch(Config-If-Ethernet1/1)#service-policy input p1
```

Configuration results

First set an ACL a1 with two items.The first item matches source IP segments 192.168.1.0/24（allowed）. The second item matches source IP segments 192.168.1.0/24 and destination IP segments 192.168.0.0/16（rejected）. Turn on QoS function in global mode and create a class-map: c1 in which matches ACL a1, and create a policy-map in which quote c1. Set the next-hop IP as 218.31.1.119 and apply the policy-map at port ethernet 1/1. After that, all messages on port ethernet 1/1 from segment 192.168.1.0/24 will be transmitted through 192.168.1.0/24 except those from 192.168.0.0/16 segment which are still be transmitted through normal L3 routing.

Chapter 2 MPLS QoS Configuration

2.1 MPLS QoS Introduction

The exp segment of MPLS（MultiProtocol Label Switch）provides the support for QoS, and hence a better service for the network communication.

2.1.1 MPLS QoS Terms

CoS：Class of Service, the class information carried in L2 802.1Q frames. It takes up 3 bits in the Tag segment of the frame header, and is called the user priority, ranging from 0 to 7.

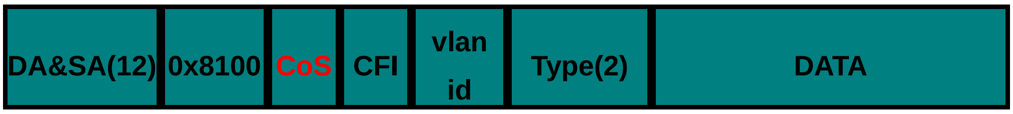


Fig 2-1 The CoS Priority

DSCP：Differentiated Services Code Point, the class information carried in L3 IP headers. It takes up 6 bits, ranging from 0 to 63, and is downward compatible with IP Precedence.

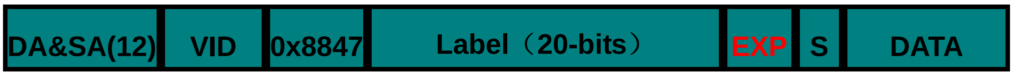


Fig 2-2 The MPLS EXP Priority

A segment in MPLS messages presenting the service class of MPLS messages. It takes up 3 bits, ranging from 0 to 7.

Internal DSCP: the internal priority configuration of the switch, used to distinguish the priorities of the switch internal data messages, ranging from 0 to 63.

In-Profile: we call the flow within the range specified by the QoS monitor policy (the bandwidth or burst value) In-Profile.

Out-of-Profile: we call the flow exceeding the range specified by the QoS monitor policy (the bandwidth or burst value) Out-of-Profile.

2.1.2 The Realization of MPLS QoS

To realize QoS of L3 switch software, a universal and mature reference model is a prerequisite. QoS can’t create any new bandwidth, but it can adjust and configure the existing bandwidth resource to achieve the maximum efficiency. A complete applicable QoS can fully control and manage the network data transmission.

The MPLS QoS based on differentiated services will specify a priority for every packet at the entrance of the network. Such class information will be stored in the exp filed of the label. MPLS

QoS provides same services to packets at the same priority level, and different services for packets with different priority. The switches or routers supporting MPLS QoS can provide different bandwidth to packets according to their class information, overwrite the class information of packets according to the monitor policy configuration and even drop some low-level packets when the bandwidth resource is tight.

2.2 MPLS QoS Configuration

The configuration task sequence of MPLS QoS is as follows:

1. Configure the class map

After creating a class rule, such as matching according to exp, the switch will treat data flow of different classes with different policies.

2. Configure the policy map

After dividing the data flow into classes, users can create a policy map corresponding with an existing class-map, and enter the policy-map mode to set the exp filed of mpls messages. They can also define an aggregate policy which can be used by multiple policy class maps in the same policy map.

3. Apply MPLS QoS to the Interface

Set the trust mode of the interface as exp, or bind the policy. The polity can only take effect on a specific interface after being bound to the latter.

4. Configure the map relationship of MPLS QoS

Configure the map from exp to dscp and that from dscp to exp.

１． **Configure the match rule of the class map as exp**

Command	Explanation
Global Configuration Mode	
match mpls-experimental topmost <exp-value-list> **no match mpls-experimental topmost**	Configure the class map to match the exp segment in the topmost label of MPLS messages.

２． **Configure the policy map**

Command	Explanation
Global Configuration Mode	
set mpls-experimental-imposition <exp-value> **no set mpls-experimental-imposition**	Policy map set the MPLS EXP value and the internal DSCP.

3． Apply QoS to an interface

Command	Explanation

Interface Configuration Mode	
mls qos mpls trust exp **no mls qos mpls trust**	Set the switch interface to trust exp; the no operation will disable this trust state of the switch interface.
mls qos cos {<*default-cos*> } **no mls qos cos**	Set the default CoS value of the switch interface; the no operation will restore the default value.

4. Configure the MPLS QoS map

Command	Explanation
Global Configuration Mode	
mls qos map {exp-dscp <*dscp1...dscp8*> | dscp-exp <*dscp-list*> to <*exp*> }	Set the Exp-to-DSCP map and the DSCP-to-Exp map

2.3 MPLS QoS Commands

2.3.1 match

Command: match mpls-experimental topmost <exp-value-list>
no match mpls-experimental topmost

Function: Set the match rules of the class map; the no operation will delete the specified match rule.

Parameters: <exp-value-list> the list of EXP value, containing at most 8 values, ranging from 0 to 7.

Default: No match rule by default.

Command Mode: Class-map Configuraiton Mode.

Usage Guide: This configuraiton only applies to MPLS messages. If this command is implemented more than once, only the last one will take effect.

Example: Create a class-map under the name of "cl" and set the match rule of this class-map as matching the EXP value 0 and 1 in the topmost label of MPSL messages.

```
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match mpls-experimental topmost 0 1
Switch(Config-ClassMap-c1)#exit
```

2.3.2 set

Command: set mpls-experimental-imposition <exp-value>
no set mpls-experimental-imposition

Function: Impose a new EXP value for the classified MPLS message; the no operation will cancel this value.

Parameters: <exp-value>the EXP value in the MPLS message, ranging from 0 to 7.

Default: No imposition by default.

Command Mode: Policy Map Configuration Mode.

Usage Guide: This configuration only applies to MPLS messages, and can only work together with class maps whose match rule is COS or EXP.

Example: Set the EXP value of messages satisfying the match rule of “c1”.

```
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set mpls-experimental-imposition 3
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
```

2.3.3 mls qos mpls trust

Command: mls qos mpls trust exp

no mls qos trust

Function: Set the interface to trust the MPSL EXP value; the no operation will disable the trust state of the switch interface.

Parameters: exp: configure the interface to trust the EXP value;

Default: the interface doesn’t trust the EXP of MPLS messages.

Command Mode: Interface Configuration Mode.

Usage Guide: The “mls qos mpls trust exp”command and the “mls qos trust dscp|cos|ip precedence”command are mutually exclusive. An interface trusting exp can’t be configured with any policy map.

Examples: Configure the interface ethernet1/1 to trust exp, which means to classify the messages according to their exp values.

```
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#mls qos mps trust exp
```

2.3.4 mls qos map

Command: mls qos map {exp-dscp <*dscp1...dscp8*> | dscp-exp <*dscp-list*> to <*exp*>}

no mls qos map {exp-dscp | dscp-exp }

Function: Set the map from exp to the internal dscp, and the map from the internal dscp to exp.

Parameters: exp-dscp <dscp1…dscp8> define the map from the CoS value to the internal DSCP, ***<dscp1...dscp8>*** are 8 internal DSCP values, separately corresponding with the EXP value 0 ~ 7. Internal DSCP values, ranging from 0 to 63, are separated from each other with spaces; **dscp-exp <*dscp-list*> to <*exp*>** defines the map from the internal DCSP value to the EXP value. ***<dscp-list>*** is the list of internal DSCP values, containing at most 8 values, ***<exp>*** is the EXP values corresponding with the DSCP values in the list.

Default: The default map is:

Default EXP-to-DSCP Map

EXP Value	0	1	2	3	4	5	6	7
DSCP Value	0	8	16	24	32	40	48	56

Default DSCP-to-EXP Map

DSCP Value	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
EXP Value	0	1	2	3	4	5	6	7

Command Mode: Global Configuration Mode.

Usage Guide: there are 64 internal dscp values, and 8 internal chip precedence levels, as a result, the dscp-exp map should map 8 consecutive dscp values to a same exp.

Example: Change the EXP-to-DSCP map from the default 0 8 16 24 32 40 48 56 to 0 1 2 3 4 5 6 7.

```
Switch(config)#mls qos map exp-dscp 0 1 2 3 4 5 6 7
```

2.3.5 show mls qos maps

Command: show mls qos maps [exp-dscp | dscp-exp|]

Function: Display the map configuration information of MPLS QoS.

Parameters: exp-dscp the map from the EXP values to the internal DSCP values; **dscp-exp** the map from the internal DSCP values to the EXP values;

Default Settings: None.

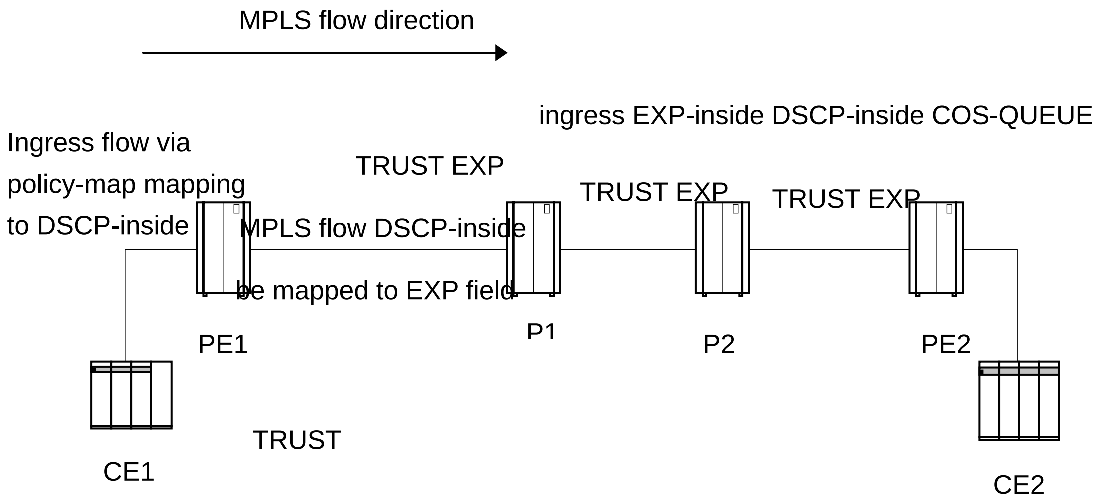
Command Mode: Admin Configuration Mode.

Usage Guide: Display the map configuration information of MPLS QoS.

Examples:

```
Switch # show mls qos maps exp-dscp
Exp-dscp map:
          exp:    0    1    2    3    4    5    6    7
-----------------------------------------------------------------
         dscp:    0    8   16   24   32   40   48    56
```

2.4 MPLS QoS Examples



According to the diff-serv QOS model, the edge switch will classify the flow, and the core switch will forward the data packets according to their classes. As demonstrated in the above figure, the edge switch PE classifies the data flow according to the policy map, and sets the exp to store the result class in MPLS messages. The following switches P and PE, which are in the state of “trust EXP”, will forward the flow.

Configuration Examples:

Assume that normal data flows enter PE1 via vlan10, voip flows enter PE1 via vlan100, and the flows enter through Ethernet 1/1 and leave from Ethernet 1/2.

PE1：

```
Switch#config
Switch(config)#mls qos
Switch(config)#class-map voip
Switch(Config-ClassMap-c1)#match vlan 100
Switch(Config-ClassMap-c1)# exit
Switch(config)#class-map data
Switch(Config-ClassMap-c1)#match vlan 10
Switch(Config-ClassMap-c1)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class voip
Switch(Config-PolicyMap-p1-Class-c1)#set mpls-experimental-imposition 1
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#class data
Switch(Config-PolicyMap-p1-Class-c1)#set mpls-experimental-imposition 0
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#service-policy input p1
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#wrr-queue bandwidth 1:1:2:2:4:4:8:8
```

Data flows, whose EXP is 0 and internal DCSP is 0, leave from queue1 according to the default DSCP－COS－QUEUE.

Voip flows, whose EXP is 1 and internal DCSP is 8, eave from queue2 according to the default DSCP－COS－QUEUE.

P1, P2, PE2: will be forwarded according to their classes, all flows will enter through Ethernet 1/1 and leave from Ethernet 1/2.

```
Switch#config
Switch(config)#mls qos
Switch(config)#interface ethernet 1/1
Switch Config-If-Ethernet1/1)#mls qos mpls trust exp
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#wrr-queue bandwidth 1:1:2:2:4:4:8:8
```

Data flows, whose EXP is 0 and internal DCSP is 0, leave from queue1 according to the default DSCP－COS－QUEUE.

Voip flows, whose EXP is 1 and internal DCSP is 8, eave from queue2 according to the default DSCP－COS－QUEUE.

```
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(Config-ClassMap-c1)#match access-group 1
Switch(Config-ClassMap-c1)# exit
Switch(config)#policy-map p1
Switch(Config-PolicyMap-p1)#class c1
Switch(Config-PolicyMap-p1-Class-c1)#set ip precedence 5
Switch(Config-PolicyMap-p1-Class-c1)#exit
Switch(Config-PolicyMap-p1)#exit
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#service-policy input p1
```

The QoS Configuration of Switch 2:

```
Switch#config
Switch(config)#mls qos
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)#mls qos trust ip-precedence pass-through-qos
```

2.5 MPLS QoS Troubleshooting Help

- ☞ The MPLS should be enabled on the switch port otherwise the MPLS QoS will be unavailable.
- ☞ After passing an interface with MPLS QoS enabled, the cos value of MPLS messages will be set to 0 while dscp will stay the same.

Chapter 3 IPv6 PBR Configuration

3.1 Introduction to PBR(Policy-based Router)

Policy-based routing provides a more powerful control over the forwarding and store of messages than traditional routing protocol to network managers. Traditionally, routers use the routing table derived from router protocol, and forward according to destination addresses. The policy-based router is more powerful and more flexible than the traditional one, because it enables network managers to choose the forwarding route not only according to destination addresses but also the size of messages, or source IP addresses. Policy can be defined as according to the balance of load in multiple routers or according to the quality of service (QOS) of the total flow forwarded in each line.

PBR (Policy-Based Routing) is a method which politically specifies the next hop when forwarding a data packet according to the source address, destination address, IP priority, TOS value, source port, destination port and other information of an IP packet.

3.2 PBR Configuration Task Sequence

1. Enable PBR function
2. Configure a class-map
3. Set the match standard in the class-map
4. Configure a policy-map
5. Configure to correlate a policy and a class-map
6. Configure the next hop IPV6 address
7. Configure the port binding policy map

1. Enable PBR function

Command	**Explanation**
Global configuration mode	
mls qos **no mls qos**	Globally enable or disable PBR function

2. Configure a class-map

Command	**Explanation**
Global configuration mode	
class-map <*class-map-name*> **no class-map <*class-map-name*>**	Create or delete a class-map

3. Set the match standard in the class-map

Command	**Explanation**
class-map mode	

match ipv6 {access-group <*acl-index-or-name*>}
no match ipv6 {access-group }
	Set the match standard in the class-map

4. Configure a policy-map

Command	**Explanation**
Global configuration mode	
policy-map <*policy-map-name*> **no policy-map <*policy-map-name*>**	Create or delete a policy-map

5. Configure to correlate a policy and a class-map

Command	**Explanation**
Policy-map mode	
class <*class-map-name*> **no class <*class-map-name*>**	Correlate with a class, and enter the policy-map mode

6. Configure the next IPv6 address

Command	**Explanation**
Policy-class-map mode	

set {ipv6 nexthop <*nexthop-ip*>}
no set {ipv6 nexthop}
	Set the next hop IPv6 address of the classed flow

7. Configure the port binding policy-map

Command	**Explanation**
Port configuration mode	

service-policy {input <*policy-map-name*> | output <*policy-map-name*>}
no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}
	Configuring the trust state of a port is mutually exclusive to applying policy-map on a port, if you want a new configuration, the former one must be deleted; there can be only one policy-map on each direction of a port. The output policy-map is not supported at present.

3.3 IPv6 PBR Function Commands

3.3.1 mls qos

Command：mls qos

no mls qos

Function：Globally enable QoS, then PBR will be enabled too. The no mls qos will globally disable QoS, PBR will be disabled too.

Command Mode：Global configuration mode.

Default：Disable PBR.

Usage Guide：While enabling and disabling QoS function, PBR function will automatically enabled and disabled. PBR can not be enabled or disabled alone.

Example：Enable and disable QoS and PBR function.

```
Switch(config)#mls qos
```

3.3.2 class-map

Command：class-map <*class-map-name*>

no class-map <*class-map-name*>

Function：Create a class-map, enter class-map mode; the **no class-map <*class-map-name*>** will delete the specified class-map.

Parameters：<*class-map-name*> the name of the class-map.

Default：There is no class-map by default.

Command Mode：Global configuration mode.

Usage Guide：None.

Example：Create and delete a class-map named as c1.

```
Switch(config)#class-map c1
Switch(config-ClassMap)#exit
Switch(config)#no class-map c1
```

3.3.3 match ipv6 access-group

Command：match ipv6 {access-group <*acl-index-or-name*>}

no match ipv6 {access-group }

Function：Set the match standard in the class-map; the **no match ipv6 {access-group }** will delete the specified match standard.

Parameters：access-group <*acl-index-or-name*> match the specified ACL list, the parameter is the index or name of the ACL.

Default：There is no match standard by default.

Command Mode：class-map mode.

Usage Guide：There can only be one match standard in each class-map. For the ACL list applied in PBR, the permit action and denies action in the entries means specify or don’t specify the next hop for the IPv6 message meeting the match standard.

Example：Create a class-map named as c1, set the classing rule of this class-map as matching the messages whose **access-group** is a1.

```
Switch(config)#class-map c1
Switch(config-ClassMap)#match ipv6 access-group a1
Switch(config-ClassMap)#exit
```

3.3.4 policy-map

Command：**policy-map <*policy-map-name*>**

no policy-map <*policy-map-name*>

Function：Create a policy-map and enter policy-map mode, the **no policy-map <*policy-map-name*>** will delete the specified policy-map.

Parameters：**<*policy-map-name*>** the name of the policy-map.

Default：There is no policy-map by default.

Command Mode：Global configuration mode.

Usage Guide：After entering policy-map mode, users can do a series of operations like the class match of PBR or setting the next hop and so on.

Examples：Create and delete a policy-map named as p1.

```
Switch(config)#policy-map p1
Switch(config-PolicyMap)#exit
Switch(config)#no policy-map p1
```

3.3.5 class

Command：**class <*class-map-name*>**

no class <*class-map-name*>

Function：Correlate a class, and enter policy-class-map mode; the **no class <*class-map-name*>**will delete the specified policy-class-map.

Parameters：**<*class-map-name*>** specify the class-map name adopted by the policy-class-map.

Default：There is no policy-class-map by default.

Command Mode：Policy-class-map mode.

Usage Guide：Before creating a policy-class-map, users should create a policy-map and enter policy-map mode first. In policy-class-map mode, users can class the packet flows classed according to the class-map and configure the next hop for them.

Example：Enter a policy-class-map mode.

```
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config-PolicyMap-Class)#exit
```

3.3.6 set

Command：set {ipv6 nexthop <*nexthop-ip*>}

no set {ipv6 nexthop}

Function：Set the next hop IP for the classed flows, the **no set {ipv6 nexthop}** will cancel the new set value.

Parameters：<*nexthop-ip*> the next hop IP, which has to be a global trunk unicast address.

Default：There is no configuration by default.

Command Mode：Policy-class-map mode.

Usage Guide：The policy of setting the next hop IP can only adopt the class-map matching IPv6 ACL.

Example：Set the next hop of the messages meeting c1 classing rules as 3ffe:506::.

```
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config-PolicyMap-Class)#set ip nexthop 3ffe:506::
Switch(config-PolicyMap-Class)#exit
Switch(config-PolicyMap)#exit
```

3.3.7 service-policy

Command：service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

no service-policy {input <*policy-map-name*> | output <*policy-map-name*>}

Function：Apply a policy-map on a switch port; the no operation of this command will delete a specified policy-map applied to the switch port.

Parameters：input <*policy-map-name*> applies the policy-map with the specified name to the input of the switch port; **output <*policy-map-name*>** applies the policy-map with the specified name to the output of the switch port.

Default：There is no bound policy-map by default.

Command Mode：Port configuration mode.

Usage Guide：Configuring the trust state of a port is mutually exclusive to applying policy-map on a port, the later configuration will overwrite the former one; there can be only one policy-map on each direction of a port. The output policy-map is not supported at present.

Example：Bind policy p1 to the input of ethernet 1/1.

```
Switch(config)#interface ethernet 1/1
Switch(Config-If-Ethernet1/1)# service-policy input p1
```

3.4 PBR Examples

Example 1：

On port ethernet 1/1, set the messages whose source IP is within the segment 2000::1/64 to do policy routing, the next hop is 3100::2.

The following is the configuration steps:

```
Switch#config
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 2000::1/64
Switch(Config-if-Vlan1)#ipv6 neighbor 2000::2 00-00-00-00-00-01 interface Ethernet 1/1
Switch(config)#interface vlan 2
Switch(Config-if-Vlan2)#ipv6 address 3000::1/64
Switch(Config-if-Vlan2)#ipv6 neighbor 3000::2 00-00-00-00-00-02 interface Ethernet 1/2
Switch(config)#interface vlan 3
Switch(Config-if-Vlan3)#ipv6 address 3100::1/64
Switch(Config-if-Vlan3)#ipv6 neighbor 3100::2 00-00-00-00-00-03 interface Ethernet 1/5
Switch(config)#ipv6 access-list extended b1
Switch(Config-IPv6-Ext-Nacl-b1)# permit tcp 2000::1/64 any-destination
Switch(Config-IPv6-Ext-Nacl-b1)#exit
Switch(config)#mls qos
Switch(config)#class-map c1
Switch(config-ClassMap)#match ipv6 access-group b1
Switch(config-ClassMap)#exit
Switch(config)#policy-map p1
Switch(config-PolicyMap)#class c1
Switch(config-Policy-Class)#set ipv6 nexthop 3100::2
Switch(config--Policy-Class)#exit
Switch(config-PolicyMap)#exit
Switch(config)#interface ethernet 1/1
Switch(Config-Ethernet1/1)#service-policy input p1
```

The configuration result:

First, set an ACL containing one entry, names it as b1, matching source IP segment 2000::1/64(permit). Globally enable QoS function, create a class-map:c1, and match ACL b1 in the class-map. Create a policy-map:p1, quoting c1 in p1, and set the next hop as 3100::2. Apply this policy-map on port ethernet 1/1. After that, the messages whose source IP are within the segment 2000::1/64 received on port ethernet 1/1 will be forwarded through 3100::2.

3.5 PBR Troubleshooting Help

- ☞ At present, policy-map can only be bound to input port but not output port.
- ☞ Since hardware resources are limited, if the policy is too complicated to configure, relative information will be noticed to users.

Chapter 4 ACL Configuration

4.1 Introduction to ACL

ACL (Access Control List) is an IP packet filtering mechanism employed in switches, providing network traffic control by granting or denying access the switches, effectively safeguarding the security of networks. The user can lay down a set of rules according to some information specific to packets, each rule describes the action for a packet with certain information matched: “permit” or “deny”. The user can apply such rules to the incoming direction of switch ports, so that data streams in the incoming direction of specified ports must comply with the ACL rules assigned.

4.1.1 Access-list

Access-list is a sequential collection of conditions that corresponds to a specific rule. Each rule consist of filter information and the action when the rule is matched. Information included in a rule is the effective combination of conditions such as source IP, destination IP, IP protocol number and TCP port, UDP port. Access-lists can be categorized by the following criteria:

- ☞ Filter information based criterion: IP access-list (layer 3 or higher information), MAC access-list (layer 2 information), and MAC-IP access-list (layer 2 or layer 3 or higher).
- ☞ Configuration complexity based criterion: standard and extended, the extended mode allows more specific filtering of information.
- ☞ Nomenclature based criterion: numbered and named.

Description of an ACL should cover the above three aspects.

4.1.2 Access-group

When a set of access-lists are created, they can be applied to traffic of incoming direction on all ports. Access-group is the description to the binding of an access-list to the incoming direction on a specific port. When an access-group is created, all packets from in the incoming direction through the port will be compared to the access-list rule to decide whether to permit or deny access.

The current firmware only supports ingress ACL configuration.

4.1.3 Access-list Action and Global Default Action

There are two access-list actions and default actions: “permit” or “deny”

The following rules apply:

- ☞ An access-list can consist of several rules. Filtering of packets compares packet conditions to the rules, from the first rule to the first matched rule; the rest of the rules will not be processed.
- ☞ Global default action applies only to IP packets in the incoming direction on the ports.
- ☞ Global default action applies only when packet flirter is enabled on a port and no ACL is bound to that port, or no binding ACL matches.

4.2 ACL Configuration

4.2.1 ACL Configuration Task Sequence

1. Configuring access-list

    （1） Configuring a numbered standard IP access-list

    （2） Configuring a numbered extended IP access-list

    （3） Configuring a standard IP access-list based on nomenclature

    a) Create a standard IP access-list based on nomenclature

    b) Specify multiple “permit” or “deny” rule entries.

    c) Exit ACL Configuration Mode

    （4） Configuring an extended IP access-list based on nomenclature.

    a) Create an extensive IP access-list based on nomenclature

    b) Specify multiple “permit” or “deny” rule entries.

    c) Exit ACL Configuration Mode

    （5） Configuring a numbered standard MAC access-list

    （6） Configuring a numbered extended MAC access-list

    （7） Configuring a extended MAC access-list based on nomenclature

    a) Create a extensive IP access-list based on nomenclature

    b) Specify multiple “permit” or “deny” rule entries.

    c) Exit ACL Configuration Mode

    （8） Configuring a numbered extended MAC-IP access-list

    （9） Configuring a extended MAC-IP access-list based on nomenclature

    a) Create a extensive MAC-IP access-list based on nomenclature

    b) Specify multiple “permit” or “deny” rule entries.

    c) Exit MAC-IP Configuration Mode

    （10） Configuring a numbered standard IPV6 access-list

    （11） Configuring a numbered extended IPV6access-list

    （12） Configuring a standard IPV6 access-list based on nomenclature

    a) Create a standard IPV6 access-list based on nomenclature

    b) Specify multiple “permit” or “deny” rule entries.

    c) Exit ACL Configuration Mode

（13） Configuring an extended IPV6 access-list based on nomenclature.

   a) Create an extensive IPV6 access-list based on nomenclature
   b) Specify multiple “permit” or “deny” rule entries.
   c) Exit ACL Configuration Mode

2. Configuring the packet filtering function
   (1) Enable global packet filtering function
   (2) Configure default action.
3. Configuring time range function
   (1) Create the name of the time range
   (2) Configure periodic time range
   (3) Configure absolute time range
4. Bind access-list to a incoming direction of the specified port.
5. Clear the filting information of the specificed port

1. Configuring access-list

(1) Configuring a numbered standard IP access-list

Command	**Explanation**
Global Mode	
access-list *<num>* {deny | permit} {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} **no access-list *<num>***	Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list; the “**no access-list *<num>***“ command deletes a numbered standard IP access-list.

(2) Configuring a numbered extensive IP access-list

Command	**Explanation**
Global Mode	
access-list *<num>* {deny | permit} icmp {{*<sIpAddr>* *<sMask>*} | any-source | {host-source *<sIpAddr>*}} {{*<dIpAddr>* *<dMask>*} | any-destination | {host-destination *<dIpAddr>*}} [*<icmp-type>* [*<icmp-code>*]] [precedence *<prec>*] [tos *<tos>*][time-range*<time-range-name>*]	Creates a numbered ICMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.

access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered IGMP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered TCP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered UDP extended IP access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | < *protocol-num* >} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered IP extended IP access rule for other specific IP protocol or all IP protocols; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
no access-list <*num*>	Deletes a numbered extensive IP access-list

(3) Configuring a standard IP access-list basing on nomenclature

a. Create a name-based standard IP access-list

Command	**Explanation**
Global Mode	

access-list ip standard <name> **no access-list ip standard <name>**	Creates a standard IP access-list based on nomenclature; the "**no access-list ip standard <name>** " command delete the name-based standard IP access-list

b. Specify multiple "permit" or "deny" rules

Command	**Explanation**
Standard IP ACL Mode	
[no] {deny | permit} {{<*sIpAddr*> <*sMask* >} | any-source | {host-source <*sIpAddr*>}}	Creates a standard name-based IP access rule; the "**no**" form command deletes the name-based standard IP access rule

c. Exit name-based standard IP ACL configuration mode

Command	**Explanation**
Standard IP ACL Mode	
exit	Exits name-based standard IP ACL configuration mode

(4) Configuring an name-based extended IP access-list

a. Create an extended IP access-list basing on nomenclature

Command	**Explanation**
Global Mode	
access-list ip extended <name> **no access-list ip extended <name>**	Creates an extended IP access-list basing on nomenclature; the "**no access-list ip extended <name>** " command deletes the name-based extended IP access-list

b. Specify multiple "permit" or "deny" rules

Command	**Explanation**
Extended IP ACL Mode	

[no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based ICMP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based IGMP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based TCP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based UDP IP access rule; the "**no**" form command deletes this name-based extended IP access rule
[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | < *protocol-num* >} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based IP access rule for other IP protocols; the "**no**" form command deletes this name-based extended IP access rule

c. Exit extended IP ACL configuration mode

Command	**Explanation**

Extended IP ACL Mode	
exit	Exits extended name-based IP ACL configuration mode

(5) Configuring a numbered standard MAC access-list

Command	**Explanation**
Global Mode	
access-list<*num*>{deny|permit}{any-source-mac|{ host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} **no access-list <*num*>**	Creates a numbered standard MAC access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list <*num*>**" command deletes a numbered standard MAC access-list.

(6) Creates a numbered MAC extended access-list

Command	**Explanation**
Global Mode	
access-list<*num*> {deny|permit} {any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[{untagged-eth2|tagged-eth2|untagged-802-3|tagged-802-3}[<*offset1*><*length1*><*value1*>[<*offset2*><*length2*><*value2*>[<*offset3*><*length3*><*value3*> [<*offset4*> <*length4*> <*value4*>]]]]] **no access-list <*num*>**	Creates a numbered MAC extended access-list, if the access-list already exists, then a rule will add to the current access-list; the "**no access-list <*num*>**" command deletes a numbered MAC extended access-list.

(7) Configuring a extended MAC access-list based on nomenclature

a. Create a extensive IP access-list based on nomenclature

Command	**Explanation**
Global Mode	

mac-access-list extended <*name*> **no mac-access-list extended <*name*>**	Creates an extended name-based MAC access rule for other IP protocols; the “**no**” form command deletes this name-based extended MAC access rule

b. **Specify multiple “permit” or “deny” rule entries**

Command	**Explanation**
Extended name-based MAC access rule Mode	
[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [cos <*cos-val*> [<*cos-bitmask*>][vlanid <*vid-value*> [<*vid-mask*>][ethertype <*protocol*> [<*protocol-mask*>]]]] **[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [ethertype <*protocol*> [<*protocol-mask*>]]** **[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [vlanid <*vid-value*> [<*vid-mask*>][ethertype <*protocol*> [<*protocol-mask*>]]]**	Creates an extended name-based MAC access rule matching MAC frame; the “**no**” form command deletes this name-based extended MAC access rule

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[untagged-eth2 [ethertype <*protocol*> [protocol-mask]]]	Creates an extended name-based MAC access rule matching untagged ethernet 2 frame; the "**no**" form command deletes this name-based extended MAC access rule
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [untagged-802-3]	Creates an MAC access rule matching 802.3 frame; the "**no**" form command deletes this MAC access rule
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[tagged-eth2 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype<*protocol*> [<*protocol-mask*>]]]	Creates an MAC access rule matching tagged ethernet 2 frame; the "**no**" form command deletes this MAC access rule
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [tagged-802-3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]	Creates an MAC access rule matching tagged 802.3 frame;the "**no**" form command deletes this MAC access rule

c. Exit ACL Configuration Mode

Command	**Explanation**
Extended name-based MAC access configure Mode	
exit	Quit the extended name-based MAC access configure mode

(8) Configuring a numbered extended MAC-IP access-list

Command	**Explanation**
Global mode	

access-list<*num*>{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}{{<*destination*><*destination-wildcard*>}|any-destination|{host-destination<*destination-host-ip*>}}[<*icmp-type> [*<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered mac-icmp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<*num*>{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}{{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}}[<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered mac-igmp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<num>{deny|permit}{any-source-mac|{host-source-mac<host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}}[s-port {<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<destination><destination-wildcard>}|any-destination| {host-destination <destination-host-ip>}}[d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<*time-range-name*>]	Creates a numbered mac-icmp extended mac-tcp access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.

access-list<*num*>{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}[s-port {<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<*destination*> <*destination-wildcard*>}|any-destination|{host-destination<*destination-host-ip*>}} [d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered mac-icmp extended mac-ip access rule; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
access-list<*num*>{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}}{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}{{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates a numbered extended mac-ip access rule for other specific mac-ip protocol or all mac-ip protocols; if the numbered extended access-list of specified number does not exist, then an access-list will be created using this number.
no access-list <*num*>	Deletes this nunbered extended MAC-IP access rule

(9) Configuring a extended MAC-IP access-list based on nomenclature

a. Create a extensive MAC-IP access-list based on nomenclature

Command	**Explanation**
Global Mode	
mac-ip-access-list extended <*name*> **no mac-ip-access-list extended <*name*>**	Creates an extended name-based MAC-IP access rule; the “**no**” form command deletes this name-based extended MAC-IP access rule

b. Specify multiple "permit" or "deny" rule entries

Command	**Explanation**
Extended name-based MAC-IP access Mode	
[no]{deny|permit} {any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination <*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>][tos<*tos*>][time-range<*time-range-name*>]	Creates an extended name-based MAC-ICMP access rule; the "**no**" form command deletes this name-based extended MAC-ICMP access rule
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination <*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based MAC-IGMP access rule; the "**no**" form command deletes this name-based extended MAC-IGMP access rule

[no]{deny|permit}{any-source-mac|{host-source-mac <host_smac>}|{<smac><smac-mask>}}{any-destination-mac|{host-destination-mac <host_dmac>}|{<dmac><dmac-mask>}}tcp {{<source><source-wildcard>}|any-source|{host-source<source-host-ip>}}[s-port {<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<destination><destination-wildcard>}|any-destination|{host-destination <destination-host-ip>}} [d-port {<*port3*> | range <*sPortMin*> <*sPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence <precedence>] [tos <tos>][time-range<*time-range-name*>]	Creates an extended name-based MAC-TCP access rule; the "**no**" form command deletes this name-based extended MAC-TCP access rule
[no]{deny|permit}{any-source-mac|{host-source-mac <*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}[s-port {<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination <*destination-host-ip*>}} [d-port {<*port3*> | range <*sPortMin*> <*sPortMax*>}] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]	Creates an extended name-based MAC-UDP access rule; the "**no**" form command deletes this name-based extended MAC-UDP access rule
[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}}{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}{{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}}[precedence<*precedence*>][tos<*tos*>][time-range<*time-range-name*>]	Creates an extended name-based access rule for the other IP protocol; the "**no**" form command deletes this name-based extended access rule

c. Exit MAC-IP Configuration Mode

Command	**Explanation**
Extended name-based MAC-IP access Mode	
exit	Quit extended name-based MAC-IP access mode

（10）Configuring a numbered standard IPV6 access-list

Command	**Explanation**
Global Mode	
ipv6 access-list <*num*> {deny | permit} {{<*sIPv6Addr*> <*sPrefixlen*>} | any-source | {host-source <*sIpv6Addr*>}} **no ipv6 access-list <*num*>**	Creates a numbered standard IPV6 access-list, if the access-list already exists, then a rule will add to the current access-list; the “**no access-list <*num*>**“ command deletes a numbered standard IP access-list.

（11） Configuring a numbered extensive IPV6 access-list

Command	**Explanation**
Global Mode	
ipv6 access-list <*num-ext*> {deny | permit} icmp {{<*sIPv6Prefix/sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [<*icmp-type*> [<*icmp-code*>]] [dscp <*dscp*>] [flow-label <*flowlabel*>]	Creates a numbered extended IPV6 access-list, if the access-list already exists, then a rule will add to the current access-list; the “**no ipv6 access-list <*num*>**“ command deletes a numbered standard IPV6 access-list.
ipv6 access-list <*num-ext*> {deny | permit} tcp {{<*sIPv6Prefix/*<*sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{< *dIPv6Prefix/*<*dPrefixlen*>} | any-destination | {host-destination <*dIPv6Addr*>}} [dPort {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [syn | ack | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label <*flowlabel*>]	

ipv6 access-list <*num-ext*> {deny | permit} udp {{<*sIPv6Prefix/<sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIPv6Prefix/<dPrefixlen*>} | any-destination | {host-destination <*dIPv6Addr*>}} [dPort {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [dscp <*dscp*>] [flow-label <*flowlabel*>]	
ipv6 access-list <*num-ext*> {deny | permit} <*next-header*> {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [dscp <*dscp*>] [flow-label < *flowlabel* >]	
no ipv6 access-list <*num*>	

（12）Configuring a standard IPV6 access-list based on nomenclature

a. Create a standard IPV6 access-list based on nomenclature

Command	**Explanation**
Global Mode	
ipv6 access-list standard <*name*> **no ipv6 access-list standard <*name*>**	Creates a standard IP access-list based on nomenclature; the "**no ipv6 access-list standard <name>** " command delete the name-based standard IPV6 access-list.

b. Specify multiple "permit" or "deny" rules

Command	**Explanation**
Standard IPV6 ACL Mode	
[no] {deny | permit} {{<*sIPv6Prefix/sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}}	Creates a standard name-based IPV6 access rule; the "**no**" form command deletes the name-based standard IPV6 access rule.

c. Exit name-based standard IP ACL configuration mode

Command	**Explanation**
Standard IPV6 ACL Mode	

exit	Exits name-based standard IPV6 ACL configuration mode.

（13）Configuring an name-based extended IPV6 access-list

a. Create an extended IPV6 access-list basing on nomenclature

Command	**Explanation**
Global Mode	
ipv6 access-list extended ***<name>*** **no ipv6 access-list extended** ***<name>***	Creates an extended IPV6 access-list basing on nomenclature; the “**no ipV6 access-list extended <name>** “ command deletes the name-based extended IPV6 access-list.

b. Specify multiple “permit” or “deny” rules

Command	**Explanation**
Extended IPV6 ACL Mode	
[no] {deny | permit} icmp {{<*sIPv6Prefix/sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [<*icmp-type*> [<*icmp-code*>]] [dscp <*dscp*>] [flow-label <*flowlabel*>]	Creates an extended name-based ICMP IPv6 access rule; the “**no**” form command deletes this name-based extended IPv6 access rule.
[no] {deny | permit} tcp {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [syn | ack | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label <*flowlabel*>]	Creates an extended name-based TCP IPV6 access rule; the “**no**” form command deletes this name-based extended IPV6 access rule.
[no] {deny | permit} udp {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [d-port	Creates an extended name-based UDP IPV6 access rule; the “**no**” form command deletes this name-based extended IPV6 access rule.

{<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [dscp <*dscp*>] [flow-label<*flowlabel*>]	
[no] {deny | permit} <*proto*> {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [dscp <*dscp*>] [flow-label<*flowlabel*>]	Creates an extended name-based IPV6 access rule for other IPV6 protocols; the “**no**” form command deletes this name-based extended IPV6 access rule.

c. Exit extended IPv6 ACL configuration mode

Command	**Explanation**
Extended IPV6 ACL Mode	
exit	Exits extended name-based IPV6 ACL configuration mode

2. Configuring packet filtering function

(1) Enable global packet filtering function

Command	**Explanation**
Global Mode	
Firewall enable	Enables global packet filtering function
Firewall disable	Disables global packet filtering function

(2) Configure default action.

Command	**Explanation**
Global Mode	
firewall default {permit |deny [ipv4|ipv6|all]}	Sets default action to “permit” or “deny”

3.Configuring time range function

（1）Create the name of the time range

Command	**Explanation**
Global Mode	
time-range <*time_range_name*>	Create a time range named *time_range_name*

no time-range <*time_range_name*>	Stop the time range function named ***time_range_name***

（2）Configure periodic time range

Command	**Explanation**
Time range Mode	
absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<*start_time*>to {Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday} <*end_time*>	Configure the time range for the request of the week,and every week will run by the time range
periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}| daily| weekdays | weekend} <*start_time*> to <*end_time*>	
[no]absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday}<*start_time*>to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday| Sunday} <*end_time*>	Stop the function of the time range in the week
[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily|weekdays|weekend} <*start_time*> to <*end_time*>	

（3）Configure absolute time range

Command	**Explanation**
Global Mode	
Absolute start<*start_time*><*start_data*>[end<*end_time*> <*end_data*>]	Configure absolute time range
[no]absolute start<*start_time*><*start_data*>[end<*end_time*><*end_data*>]	Stop the function of the time range

4. Bind access-list to a specific direction of the specified port.

Command	**Explanation**
Physical Interface Mode,Interface Mode	

{ip|ipv6|mac|mac-ip} access-group <*name*> {in}
no {ip|ipv6|mac|mac-ip} access-group <*name*> {in}
	Applies an access-list to the specified direction on the port; the "**no {ip|ipv6|mac|mac-ip} access-group <*name*> {in}**" command deletes the access-list bound to the port.

5. Clear the filting information of the specificed port

Command	**Explanation**
Admin Mode	
clear access-group statistic interface {<*interface-name*> | ethernet<*interface-name*>}	Clear the filting information of the specificed port

4.2.2 Commands for ACL

4.2.2.1 absolute-periodic/periodic

Command:

[no] absolute-periodic{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday| Sunday}<start_time>to{Monday|Tuesday|Wednesday|Thursday|Friday|Saturday| Sunday} <end_time>

[no]periodic{{Monday+Tuesday+Wednesday+Thursday+Friday+Saturday+Sunday}|daily| weekdays | weekend} <start_time> to <end_time>

Functions: Define the time-range of different commands within one week, and every week to circulate subject to this time.

Parameters:

Friday	（Friday)
Monday	（Monday)
Saturday	（Saturday)
Sunday	（Sunday)
Thursday	（Thursday）
Tuesday	（Tuesday)
Wednesday	（Wednesday)
daily	（Every day of the week）
weekdays	（Monday thru Friday）
weekend	（Saturday thru Sunday）
start_time	start time ,HH:MM:SS (hour: minute: second)

end_time end time,HH:MM:SS (hour: minute: second)

Remark: time-range polling is one minute per time, so the time error shall be <= one minute.

Command Mode: time-range mode

Default: No time-range configuration

Usage Guide: Periodic time and date. The definition of period is specific time period of Monday to Saturday and Sunday every week.

day1 hh:mm:ss To day2 hh:mm:ss or

{[day1+day2+day3+day4+day5+day6+day7]|weekend|weekdays|daily} hh:mm:ss To hh:mm:ss

Examples: Make configurations effective within the period from9:15:30 to 12:30:00 during Tuesday to Saturday.

Switch(config)#time-range test

Switch(Config-Time-Range-test)#absolute-periodic Tuesday 9:15:30 to Saturday 12:30:00

Make configurations effective within the period from 14:30:00 to 16:45:00 on Monday, Wednesday, Friday and Sunday.

Switch (Config-Time-Range-test)#periodic Monday Wednesday Friday Sunday 14:30:00 to 16:45:00

4.2.2.2 absolute start

Command:[no]absolute start <*start_time*> <*start_data*> [end <*end_time*> <*end_data*>]

Functions: Define an absolute time-range, this time-range operates subject to the clock of this equipment.

Parameters:*start_time* : start time, HH:MM:SS (hour: minute: second)

***end_time* :** end time, HH:MM:SS (hour: minute: second)

***start_data* :** start data, the format is, YYYY.MM.DD（year.month.day） ***end_data* :** end data, the format is, YYYY.MM.DD（year.month.day）

Remark: time-range is one minute per time, so the time error shall be <= one minute.

Command Mode: Time-range mode

Default: No time-range configuration

Usage Guide: Absolute time and date, assign specific year, month, day, hour, minute of the start, shall not configure multiple absolute time and date, when in repeated configuration, the latter configuration covers the absolute time and date of the former configuration.

Examples: Make configurations effective from 6:00:00 to 13:30:00 from Oct. 1, 2004 to Jan. 26, 2005.

Switch(config)#Time-range edge

Switch(Config-Time-Range-edge)#absolute start 6:00:00 2004.10.1 end 13:30:00 2005.1.26

4.2.2.3 access-list(ip extended)

Command: access-list <*num*> {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [ack+ fin+ psh+ rst+ urg+ syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list <*num*> {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | <*protocol-num*>} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

no access-list <*num*>

Functions: Create a numeric extended IP access rule to match specific IP protocol or all IP protocol; if access-list of this coded numeric extended does not exist, thus to create such a access-list.

Parameters: <*num*> is the No. of access-list, 100-299; **<*protocol*> is the No. of upper-layer protocol of ip, 0-255; <*sIpAddr*>** is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation; **<*dIpAddr*>** is the destination IP address, the format is dotted decimal notation; **<*dMask*>** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position1;**<*igmp-type*>**,the type of igmp, 0-15; **<*icmp-type*>**, the type of icmp, 0-255;**<icmp-code>,** protocol No. of icmp, 0-255;**<prec>**, IP priority, 0-7; **<*tos*>**, to value, 0-15; **<*sPort*>**, source port No., 0-65535; **<*sPortMin*>**, the down boundary of source port;； **<*sPortMax*>**, the up boundary of source port; **<*dPortMin*>**, the down boundary of destination port;**<*dPortMax*>**, the up boundary of destination port; **<*dPort*>**, destination port No., 0-65535; **<*time-range-name*>**, the name of time-range.

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific ***<num>*** for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 200-299 can configure not continual reverse mask of IP address.

<igmp-type> represent the type of IGMP packet, and usual values please refer to the following description:

17(0x11): IGMP QUERY packet

18(0x12): IGMP V1 REPORT packet

22(0x16): IGMP V2 REPORT packet

23(0x17): IGMP V2 LEAVE packet

34(0x22): IGMP V3 REPORT packet

19(0x13): DVMR packet

20(0x14): PIM V1 packet

Particular notice: the packet types included here are not the types excluding IP OPTION. Normally, IGMP packet contains OPTION fields, and such configuration is of no use for this type of packet. If you want to configure the packets containing OPTION, please directly use the manner where OFFSET is configured.

Examples: Create the numeric extended access-list whose serial No. is 110. deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

```
Switch(config)#access-list 110 deny icmp any any-destination
Switch(config)#access-list 110 permit udp any host-destination 192.168.0.1 d-port 32
```

4.2.2.4 access-list(ip standard)

Command: access-list <*num*> {deny | permit} {{<*sIpAddr*> <*sMask* >} | any-source| {host-source <*sIpAddr*>}}

no access-list <*num*>

Functions: Create a numeric standard IP access-list. If this access-list exists, then add a rule list; the "**no access-list <*num*>**" operation of this command is to delete a numeric standard IP access-list.

Parameters: ***<num>*** is the No. of access-list, 100-199; ***<sIpAddr>*** is the source IP address, the format is dotted decimal notation; ***<sMask >*** is the reverse mask of source IP, the format is dotted decimal notation;

Command Mode: Global mode

Default: No access-lists configured.

Usage Guide: When the user assign specific ***<num>*** for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Create a numeric standard IP access-list whose serial No. is 20, and permit date packets with source address of 10.1.1.0/24 to pass, and deny other packets with source address of 10.1.1.0/16.

Switch(config)#access-list 20 permit 10.1.1.0 0.0.0.255

Switch(config)#access-list 20 deny 10.1.1.0 0.0.255.255

4.2.2.5 access-list(mac extended)

Command:access-list<*num*>{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}{untagged-eth2|tagged-eth2|untagged-802-3|tagged-802-3}[<*offset1*> <*length1*> <*value1*> [<*offset2*> <*length2*> <*value2*> [<*offset3*> <*length3*> <*value3*> [<*offset4*> <*length4*> <*value4*>]]]]

no access-list <*num*>

Functions: Define a extended numeric MAC ACL rule,'**no access-list <*num*>**' command deletes an extended numeric MAC access-list rule.

Parameters:

<*num*> is the access-list No. which is a decimal's No. from 1100-1199; ***deny*** if rules are matching, deny access; ***permit*** if rules are matching, permit access; ***<any-source-mac>*** any source address; ***<any-destination-mac>*** any destination address; ***<host_smac>, <sumac>*** source MAC address; ***<sumac-mask>*** mask (reverse mask) of source MAC address; ***<host_dmac> , <dmac>*** destination MAC address; ***<dmac-mask>*** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet; **Offset(x)** the offset from the packet head, the range is (12-79), the windows must start from the back of source MAC, and the windows cannot superpose each other, and that is to say: Offset(x＋1) must **be longer than** Offset(x)＋len（x）; ***Length(x)*** length is 1-4 , and **Offset(x)＋Length(x) should not be longer than 80（currently should not be longer than 64）;** ***Value(x)*** **hex expression, Value range**: when **Length(x)** =1, it is 0-ff , when **Length(x)** =2, it is 0-ffff , when **Length(x)** =3, it is0-ffffff, when **Length(x)** =4, it is 0-ffffffff ;

For **Offset(x),** different types of data frames are with different value ranges:

for untagged-eth2 type frame: <12～52>

for untagged-802.2 type frame: <12～60>

for untagged-eth2 type frame: <12～56>

for untagged-eth2 type frame: <12～64>

Command Mode: Global mode

Default Configuration : No access-list configured

Usage Guide: When the user assign specific **<*num*>** for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets whose 15th and 16th byte is 0x08 , 0x0 to pass, and

Switch(config)#access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800

4.2.2.6 access-list(mac-ip extended)

Command:access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}icmp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}}[<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}igmp {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac| {host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}tcp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}}[s-port{<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<*destination*> <*destination-wildcard*>} | any-destination | {host-destination <*destination-host-ip*>}} [d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence <*precedence*>] [tos <*tos*>] [time-range <*time-range-name*>]

access-list<*num*>{deny|permit}{any-source-mac| {host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac| {host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}udp {{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}}[s-port{<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<*destination*><*destination-wildcard*>}|any-destination| {host-destination<*destination-host-ip*>}}[d-port{<*port3*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

access-list<*num*>{deny|permit}{any-source-mac|

{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}
{any-destination-mac|{host-destination-mac <*host_dmac*>}|{<*dmac*><*dmac-mask*>}}
{eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}}
{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}}
{{<*destination*><*destination-wildcard*>}|any-destination|
{host-destination<*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Define a extended numeric MAC-IP ACL rule, 'No' command deletes a extended numeric MAC-IP ACL access-list rule.

Parameters: num access-list serial No. this is a decimal's No. from 3100-3299.; **deny** if rules are matching, deny to access; **permit** if rules are matching, permit to access; **any-source-mac**: any source MAC address; **any-destination-mac**: any destination MAC address; **host_smac , smac**: source MAC address; **smac-mask: mask** (reverse mask) of source MAC address ; **host_dmac , dmas** destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **protocol** No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list; **source-host-ip, source** No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression; host: means the address is the IP address of source host, otherwise the IP address of network; **source-wildcard**: reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **destination-host-ip**, destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression; **host:** means the address is the that the destination host address, otherwise the network IP address; **destination-wildcard**: mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; **s-port(optional)**: means the need to match TCP/UDP source port; **port1(optional)**: value of TCP/UDP source interface No., Interface No. is an integer from 0-65535; **d-port(optional)**: means need to match TCP/UDP destination interface; ***<sPortMin>***, the down boundary of source port; ***<sPortMax>***, the up boundary of source port; **port3(optional)**: value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535; ***<dPortMin>***, the down boundary of destination port;***<dPortMax>***, the up boundary of destination port; **[ack] [fin] [psh] [rst] [urg] [syn]**,(optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection; **precedence** (optional) packets can be filtered by priority which is a number from 0-7; **tos** (optional) packets can be filtered by service type which ia number from 0-15; **icmp-type** (optional) ICMP packets can be filtered by packet type which is a number from 0-255; **icmp-code** (optional) ICMP packets can be filtered by packet code which is a number from 0-255; **igmp-type** (optional) ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255; **<time-range-name>**, name of time range

Command Mode: Global mode

Default Configuration:no access-list configured

Usage Guide: When the user assign specific <num> for the first time, ACL of the serial number is created, then the lists are added into this ACL; the access list which marked 3200-3299 can configure not continual reverse mask of IP address.

Examples: Permit the passage of TCP packet with source MAC 00-12-34-45-XX-XX, any destination MAC address, source IP address 100.1.1.0 0.255.255.255, and source port 100 and destination interface 40000.

Switch(config)#access-list 3199 permit 00-12-34-45-67-00 00-00-00-00-FF-FF any-destination-mac tcp 100.1.1.0 0.255.255.255 s-port 100 any-destination d-port 40000

4.2.2.7 access-list(mac standard)

Command: access-list <*num*> {deny|permit} {any-source-mac | {host-source-mac <*host_smac*> } | {<*smac*> <*smac-mask*>} }

no access-list <num>

Functions: Define a standard numeric MAC ACL rule, '**no access-list <num>**' command deletes a standard numeric MAC ACL access-list rule

Parameters: **<*num*>** is the access-list No. which is a decimal's No. from 700-799; ***deny*** if rules are matching, deny access; ***permit*** if rules are matching, permit access; **<*host_smac*>, <*sumac*>** source MAC address; **<*sumac-mask*>** mask (reverse mask) of source MAC address

Command Mode: Global mode

Default Configuration : No access-list configured

Usage Guide: When the user assign specific **<***num***>** for the first time, ACL of the serial number is created, then the lists are added into this ACL.

Examples: Permit the passage of packets with source MAC address 00-00-XX-XX-00-01, and deny passage of packets with source MAC address 00-00-00-XX-00-ab.

Switch(config)# access-list 700 permit 00-00-00-00-00-01 00-00-FF-FF-00-01

Switch(config)# access-list 700 deny   00-00-00-00-00-ab 00-00-00-FF-00-ab

4.2.2.8 clear access-group statistic interface

Command: clear access-group statistic interface {<*interface-name*> | ethernet<*interface-name*>}

Functions: Empty packet statistics information of assigned interfaces.

Parameters:<*interface-name*>: Interface name.

Command Mode: Admin mode.

Default: None

Examples: Empty packet statistics information of interface E1/1.

Switch#clear access-group statistic interface ethernet 1/1

4.2.2.9 firewall

Command: firewall { enable | disable}

Functions: Enable or disable firewall

Parameters: enable means to enable of firewall; **disable** means to disable firewall.

Default: It is no use if default is firewall

Command Mode: Global mode

Usage Guide: Whether enabling or disabling firewall, access rules can be configured. But only when the firewall is enabled, the rules can be used in specific orientations of specific ports. When disabling the firewall, all ACL tied to ports will be deleted.

Examples: Enable firewall

Switch(config)#firewall enable

4.2.2.10 firewall default

Command: firewall default {permit | deny [ipv4|ipv6|all]}

Functions: Configure default actions of firewall

Parameters: permit means to permit data packets to pass; **deny** means to deny ipv4|ipv6|arp|all data packets to pass.

Command Mode: Global mode

Default: Default action is permit.

Usage Guide: This command only influences IP packets from the port entrance, and all packets can pass the switch in other situations.

Examples: Configure firewall default action as permitting packets to pass.

Switch(config)#firewall default permit

4.2.2.11 access-list ip

Command: access-list ip {standard | extended} <name>
no access-list ip {standard | extended} <name>

Functions: Create a name standard or extended IP access-list; **no access-list ip {standard | extended}<*name*>** action of this command deletes this name standard or extended IP access-list (including all list items);

Parameters: standard means standard IP access-list ; **extended** means extended IP access-list; **<*name*>** name the access-list, the length of character string is 1-16, no pure number sequences permitted.

Command Mode: Global mode

Default: No access-list configured

Usage Guide: After assigning this commands for the first time, only am empty name access-list is created, and no items in the list.

Examples: Create a name extended IP access-list whose name is tcpFlow.

Switch(config)# access-list ip extended tcpFlow

4.2.2.12 ipv6 access-list

Command：ipv6 access-list <*num-std*> {deny | permit} {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}}

ipv6 access-list <*num-ext*> {deny | permit} icmp {{<*sIPv6Prefix*/*sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [<*icmp-type*> [<*icmp-code*>]] [dscp <*dscp*>] [flow-label <*flowlabel*>]

ipv6 access-list <*num-ext*> {deny | permit} tcp {{<*sIPv6Prefix/*<*sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{< *dIPv6Prefix/*<*dPrefixlen*>} | any-destination | {host-destination <*dIPv6Addr*>}} [dPort {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [syn | ack | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label <*flowlabel*>]

ipv6 access-list <*num-ext*> {deny | permit} udp {{<*sIPv6Prefix/*<*sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIPv6Prefix/*<*dPrefixlen*>} | any-destination | {host-destination <*dIPv6Addr*>}} [dPort {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [dscp <*dscp*>] [flow-label <*flowlabel*>]

ipv6 access-list <*num-ext*> {deny | permit} <*next-header*> {<*sIPv6Prefix*/*sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [dscp <*dscp*>] [flow-label<*flowlabel*>]

no ipv6 access-list {<*num-std*>|<*num-ext*>}

Functions：Creates a numbered standard IP access-list, if the access-list already exists, then a rule will add to the current access-list; the “**no access-list {<*num-std*>|<*num-ext*>}** “ command deletes a numbered standard IP access-list.

Parameters：*<num-std>* is the list number ,list range is between 500～599; ***<num-ext>*** is the list number ,list range is between 600～699; ***<sIPv6Prefix>*** is the prefix of the ipv6 source address; ***<sPrefixlen >*** is the length of prefix of the ipv6 source address, range is between 1～128; ***<sIPv6Addr>*** is the ipv6 source address; ***<dIPv6Prefix>*** is the prefix of the ipv6 destination address; ***<dPrefixlen >*** is the length of prefix of the ipv6 destination address, range is between 1～128; ***<dIPv6Addr>*** is the ipv6 destination address; ***<icmp-type>***, the type of icmp; ***<icmp-code>***，the protocol code of icmp; ***<dscp>***，IPv6 priority, range from 0 to 63；

<flowlabel>，value of flow tag, range from 0 to 1048575; **syn**，**ack**，**urg**，**rst**，**fin**，**psh**，tcp 标志位； ***<sPort>***, source port No., 0-65535; ***<sPortMin>***, the down boundary of source port; ***<sPortMax>***, the up boundary of source port;***<dPort>***，destination port No., range from 0 to 65535; ***<dPortMin>***, the down boundary of destination port;***<dPortMax>***, the up boundary of destination port; ***<next-header>***，the next header of IPv6, range from 0 to 255.

Command Mode: Global mode

Default: No access-list configured

Usage Guide: Creates a numbered 520 standard IP access-list first time,the following configuration will add to the current access-list.

Examples: Creates a numbered 520 standard IP access-list,allow the source package from 2003:1:2:3::1/64 pass through the net,and deny all the other package from the source address 2003:1:2::1/48 pass through

```
Switch (config)#ipv6 access-list 520 permit 2003:1:2:3::1/64
Switch (config)#ipv6 access-list 520 deny 2003:1:2:::1/48
```

4.2.2.13 ipv6 access standard

Command: ipv6 access-list standard <*name*>

no ipv6 access-list standard <*name*>

Function: Create a name-based standard IPv6 access list; the "**no ipv6 access-list standard<*name*>**"command deletes the name-based standard IPv6 access list (including all entries).

Parameter:<*name*> is the name for access list, the character string length is from 1 to 16.

Command Mode: Global Mode

Default: No access list is configured by default

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created.

Example: Create a standard IPv6 access list named "ip6Flow"

```
Switch(config)#ipv6 access-list standard ip6Flow
```

4.2.2.14 ipv6 access extended

Command:ipv6 access-list extended <*name*>

no ipv6 access-list extended <*name*>

Function: Create a name-based extended IPv6 access list; the "**no ipv6 access-list extended<*name*>**" command delete the name-based extended IPv6 access list

Parameter:<*name*> is the name for access list, the character string length is from 1 to 16.

Command Mode: Global Mode

Default: No IP address is configured by default.

Usage Guide: When this command is run for the first time, only an empty access list with no entry will be created

Example: Create an extensive IPv6 access list named “tcpFlow”.

Switch (config)#ipv6 access-list extended tcpFlow

4.2.2.15 {ip|ipv6|mac|mac-ip} access-group

Command :{ip|ipv6|mac|mac-ip} access-group <*name*> {in}[traffic-statistic]

no {ip|mac|mac-ip} access-group <*name*> {in}

Function: Apply a access-list on some direction of port, and determine if ACL rule is added statistic counter or not by options; the “no {ip|mac|mac-ip} access-group command deletes access-list binding on the port.

Parameter: <*name*> is the name for access list, the character string length is from 1 to 16

Command Mode: Physical Interface Mode,Interface Mode

Default: The entry of port is not bound ACL.

Usage Guide: One port can bind an entry rule.

The **standard, extended and nomenclature** of access-list can be bound to **physical port** of layer 3 switch, not binding ACL to layer interface or influx interface.

There are four kinds of package head field based on concerned: MAC ACL, IP CAL, MAC-IP ACL, and IPv6 ACL; to some extent, ACL filter behavior (permit, deny) has a conflict when a data package matches multi types of eight ACLs. The strict priorities are specified for each ACL based on outcome veracity. It can determine final behavior of package filter through priority when the filter behavior has a conflict.

When binding ACL to port, there are some limits as below:

1. Each port can bind a MAC-IP ACL, a IP ACL, a MAC ACL and a IPv6 ACL;
2. When binding 6 ACLs and data package matching the multi ACLs simultaneity, the priority from high to low are shown as below,
   Ingress IPv6 AC;
   Ingress MAC-IP ACL;
   Ingress MAC ACL;
   Ingress IP ACL;

Example: Binding aaa access-list to entry direction of port

Switch(Config-If-Ethernet1/1)#ip access-group aaa in

4.2.2.16 mac-access-list extended

Command: mac-access-list extended <*name*>

no mac-access-list extended <*name*>

Functions: Define a name-manner MAC ACL or enter access-list configuration mode,**‘**no mac-access-list extended <*name*>’ command deletes this ACL.

Parameters:<name> name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 16 (remark: sensitivity on capital or small letter.)

Command Mode: Global mode

Default Configuration: No access-lists configured

Usage Guide:After assigning this commands for the first time, only an empty name access-list is created and no list item included.

Examples: Create an MAC ACL named mac_acl.

Switch(config)#mac-access-list extended mac_acl

Switch(Config-Mac-Ext-Nacl-mac_acl)#

4.2.2.17 mac-ip access extended

Command: Mac-ip-access-list extended <*name*>

no mac-ip-access-list extended <*name*>

Functions: Define a name-manner MAC-IP ACL or enter access-list configuration mode, **'no mac-ip-access-list extended <*name*>**' command deletes this ACL.

Parameters:<*name*> :name of access-list excluding blank or quotation mark, and it must start with letter, and the length cannot exceed 16 (remark: sensitivity on capital or small letter.)

Command Mode: Global mode

Default: No named MAC-IP access-list

Usage Guide:After assigning this commands for the first time, only an empty name access-list is created and no list item included.

Examples: Create an MAC-IP ACL named macip_acl

Switch(config)# mac-ip-access-list extended macip_acl

Switch(Config-MacIp-Ext-Nacl-macip_acl)#

4.2.2.18 permit | deny(ip extended)

Command: [no] {deny | permit} icmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} igmp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [<*igmp-type*>] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} tcp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [ack+fin+psh+rst+urg+syn] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} udp {{<*sIpAddr*> <*sMask*>} | any-source | {host-source

<*sIpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

[no] {deny | permit} {eigrp | gre | igrp | ipinip | ip | ospf | < *protocol-num* >} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}} {{<*dIpAddr*> <*dMask*>} | any-destination | {host-destination <*dIpAddr*>}} [precedence <*prec*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Create a name extended IP access rule to match specific IP protocol or all IP protocol;

Parameters: **<*sIpAddr*>** is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation; **<*dIpAddr*>** is the destination IP address, the format is dotted decimal notation; **<*dMask*>** is the reverse mask of destination IP, the format is dotted decimal notation, attentive position o, ignored position 1; **<*igmp-type*>**, the type of igmp, 0-15; **<*icmp-type*>**, the type of icmp, 0-255 ; **<icmp-code>,** protocol No. of icmp, 0-255; **<prec>**, IP priority, 0-7; **<*tos*>**, to value, 0-15; **<*sPort*>**, source port No., 0-65535; **<*sPortMin*>**, the down boundary of source port; **<*sPortMax*>**, the up boundary of source port; **<*dPort*>**, destination port No. 0-65535; **<*dPortMin*>**, the down boundary of destination port;**<*dPortMax*>**, the up boundary of destination port; **<*time-range-name*>**, time range name.

Command Mode: Name extended IP access-list configuration mode

Default: No access-list configured

Examples: Create the extended access-list, deny icmp packet to pass, and permit udp packet with destination address 192. 168. 0. 1 and destination port 32 to pass.

```
Switch(config)# access-list ip extended udpFlow
Switch(Config-IP-Ext-Nacl-udpFlow)# deny igmp any any-destination
Switch(Config-IP-Ext-Nacl-udpFlow)# permit udp any host-destination 192.168.0.1 d-port 32
```

4.2.2.19 permit | deny(ip standard)

Command:{deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}

no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}

Functions: Create a name standard IP access rule, and '**no {deny | permit} {{<*sIpAddr*> <*sMask*>} | any-source | {host-source <*sIpAddr*>}}**' action of this command deletes this name standard IP access rule.

Parameters: **<*sIpAddr*>** is the source IP address, the format is dotted decimal notation; **<*sMask* >** is the reverse mask of source IP, the format is dotted decimal notation;

Command Mode: Name standard IP access-list configuration mode

Default: No access-list configured

Example: Permit packets with source address 10.1.1.0/24 to pass, and deny other packets with source address 10.1.1.0/16.

Switch(config)# access-list ip standard ipFlow

Switch(Config-IP-Std-Nacl-ipFlow)# permit 10.1.1.0 0.0.0.255

Switch(Config-IP-Std-Nacl-ipFlow)# deny 10.1.1.0 0.0.255.255

4.2.2.20 permit | deny(mac extended)

Command:

[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [cos <*cos-val*> [<*cos-bitmask*>][vlanid <*vid-value*> [<*vid-mask*>][ethertype <*protocol*> [<*protocol-mask*>]]]]

[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [ethertype <*protocol*> [<*protocol-mask*>]]

[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} [vlanid <*vid-value*> [<*vid-mask*>][ethertype <*protocol*> [<*protocol-mask*>]]] [no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[untagged-eth2[ethertype<*protocol*>[protocol-mask]]]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[untagged-802-3]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[tagged-eth2[cos<*cos-val*>[<*cos-bitmask*>]][vlanId<*vid-value*>[<*vid-mask*>]][ethertype<*protocol*>[<*protocol-mask*>]]]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}}[ta

gged-802-3[cos<*cos-val*>[<*cos-bitmask*>]][vlanId<*vid-value*>[<*vid-mask*>]]]

Functions: Define an extended name MAC ACL rule, and 'no' formof this command deletes this extended name IP access rule.

Parameters: any-source-mac: any source of MAC address; **any-destination-mac**: any destination of MAC address; **host_smac , smac**: source MAC address; **smac-mask**: mask (reverse mask) of source MAC address ; **host_dmac , dmas** destination MAC address; **dmac-mask** mask (reverse mask) of destination MAC address; **untagged-eth2** format of untagged ethernet II packet; **tagged-eth2** format of tagged ethernet II packet; **untagged-802-3** format of untagged ethernet 802.3 packet; **tagged-802-3** format of tagged ethernet 802.3 packet; ***cos-val*:** cos value, 0-7; ***cos-bitmask*:** cos mask, 0-7reverse mask and mask bit is consecutive; ***vid-value*:** vlanNo, 1-4094; ***vid-bitmask* :**vlan mask, 0-4095, reverse mask and mask bit is consecutive; ***protocol*:** specific Ethernet protocol No., 1536-65535; ***protocol-bitmask*:** protocol mask, 0-65535, reverse mask and mask bit is consecutive.

Notice: mask bit is consecutive means the effective bit must be consecutively effective from the first bit on the left, no ineffective bit can be added through. For example: the reverse mask format of one byte is: 00001111b; mask format is 11110000; and this is not permitted: 00010011.

Command Mode: Name extended MAC access-list configuration mode

Default configuration: No access-list configured

4.2.2.21 permit | deny(mac-ip extended)

Command: [no] {deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} icmp{{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [<*icmp-type*> [<*icmp-code*>]] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit} {any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*><*smac-mask*>}} {any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dmac*><*dmac-mask*>}} igmp{{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [<*igmp-type*>] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}| {<*smac*><*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}|{<*dm*

_ac_><*dmac-mask*>}}tcp{{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}}[s-port {<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<*destination*> <*destination-wildcard*>} | any-destination| {host-destination <*destination-host-ip*>}} [d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [ack＋fin＋psh ＋rst＋urg＋syn] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*> <*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}| {<*dmac*><*dmac-mask*>}}udp{{<*source*><*source-wildcard*>}|any-source| {host-source<*source-host-ip*>}}[s-port{<*port1*> | range <*sPortMin*> <*sPortMax*>}] {{<*destination*> <*destination-wildcard*>}|any-destination| {host-destination <*destination-host-ip*>}} [d-port {<*port3*> | range <*dPortMin*> <*dPortMax*>}] [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

[no]{deny|permit}{any-source-mac|{host-source-mac<*host_smac*>}|{<*smac*> <*smac-mask*>}}{any-destination-mac|{host-destination-mac<*host_dmac*>}| {<*dmac*><*dmac-mask*>}}{eigrp|gre|igrp|ip|ipinip|ospf|{<*protocol-num*>}} {{<*source*><*source-wildcard*>}|any-source|{host-source<*source-host-ip*>}} {{<*destination*><*destination-wildcard*>}|any-destination|{host-destination <*destination-host-ip*>}} [precedence <*precedence*>] [tos <*tos*>][time-range<*time-range-name*>]

Functions: Define an extended name MAC-IP ACL rule, 'No' form deletes one extended numeric MAC-IP ACL access-list rule.

Parameters: num access-list serial No. this is a decimal's No. from 3100-3199.; deny if rules are matching, deny to access; permit if rules are matching, permit to access; any-source-mac: any source MAC address; any-destination-mac: any destination MAC address; host_smac , smac: source MAC address; smac-mask: mask (reverse mask) of source MAC address ; host_dmac , dmas destination MAC address; dmac-mask mask (reverse mask) of destination MAC address; protocol No. of name or IP protocol. It can be a key word: eigrp, gre, icmp, igmp, igrp, ip, ipinip, ospf, tcp, or udp, or an integer from 0-255 of list No. of IP address. Use key word 'ip' to match all Internet protocols (including ICMP, TCP, AND UDP) list; source-host-ip, source No. of source network or source host of packet delivery. Numbers of 32-bit binary system with dotted decimal notation expression; host: means the address is the IP address of source host, otherwise the IP address of network; source-wildcard: reverse of source IP. Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; destination-host-ip, destination No. of destination network or host to which packets are delivered. Numbers of 32-bit binary system with dotted decimal notation expression; host: means the address is the that the destination host address, otherwise the network IP address; destination-wildcard: mask of destination. I Numbers of 32-bit binary system expressed by decimal's numbers with four-point separated, reverse mask; s-port(optional): means the need to match TCP/UDP source port; **port1(optional):** value of TCP/UDP source interface No., Interface No. is an integer from 0-65535; ***<sPortMin>*,** the down boundary of source port; ***<sPortMax>*,** the up boundary of source port; **d-port(optional):** means need to match TCP/UDP destination interface; **port3(optional)**: value of TCP/UDP destination interface No., Interface No. is an integer from 0-65535; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port; **[ack] [fin] [psh] [rst] [urg] [syn]**, (optional) only for TCP protocol, multi-choices of tag positions are available, and when TCP data reports the configuration of corresponding position, then initialization of TCP data report is enabled to form a match when in connection; **precedence** (optional) packets can be filtered by priority which is a number from 0-7; **tos** (optional) packets can be filtered by service type which ia number from 0-15; **icmp-type** (optional) ICMP packets can be filtered by packet type which is a number from 0-255; **icmp-code** (optional) ICMP packets can be filtered by packet code which is a number from 0-255; **igmp-type** (optional) ICMP packets can be filtered by IGMP packet name or packet type which is a number from 0-255; ***<time-range-name>***, name of time range.

Command Mode: Name extended MAC-IP access-list configuration mode

Default: No access-list configured

Examples: Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100 and destination port 40000.

Switch (config)# access-list 3100 deny any-source-mac any-destination-mac udp any s-port 100 any-destination d-port 40000

4.2.2.22 permit | deny(ipv6 extended)

Command: [no] {deny | permit} icmp {{<*sIPv6Prefix*/*sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [<*icmp-type*> [<*icmp-code*>]] [dscp <*dscp*>] [flow-label <*flowlabel*>]

[no] {deny | permit} tcp {<*sIPv6Prefix*/*sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [syn | ack | urg | rst | fin | psh] [dscp <*dscp*>] [flow-label<*flowlabel*>]

[no] {deny | permit} udp {<*sIPv6Prefix*/*sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [d-port {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [dscp <*dscp*>] [flow-label <*flowlabel*>]

[no] {deny | permit} <*next-header*> {<*sIPv6Prefix*/*sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [dscp <*dscp*>] [flow-label <*flowlabel*>]

Function: Create an extended nomenclature IPv6 access control rule for specific IPv6 protocol.

Parameter:*<sIPv6Addr>* is the source IPv6 address;***<sPrefixlen>*** is the length of the IPv6 address prefix,the range is 1～128;***<dIPv6Addr>*** is the destination IPv6 address;***<dPrefixlen>*** is the length of the IPv6 address prefix,the range is 1～128;***<igmp-type>***,type of the igmp;***<icmp-type>***,icmp type;***<icmp-code>***,icmp protocol number;***<dscp>***,IPv6 priority ,the range is 0～63; ***<flowlabel>***,value of the flow label,the range is 0～1048575;**syn**,**ack**,**urg**,**rst**,**fin**,**psh**,tcp label position;***<sPort>***,source port number,the range is 0～65535; ***<sPortMin>***, the down boundary of source port; ***<sPortMax>***, the up boundary of source port; ***<dPort>***, destination port number, the range is 0～65535; ***<dPortMin>***, the down boundary of destination port; ***<dPortMax>***, the up boundary of destination port.

Command Mode: IPv6 nomenclature extended access control list mode

Default: No access control list configured

Example: Create an extended access control list named udpFlow, denying the igmp packets while allowing udp packets with destination address 2001:1:2:3::1 and destination port 32.

```
Switch(config)#ipv6 access-list extended udpFlow
Switch(Config-IPv6-Ext-Nacl-udpFlow)#ipv6 access-list 110 deny igmp any any-destination
Switch(Config-IPv6-Ext-Nacl-udpFlow)#ipv6 access-list 110 permit udp any host-destination 2001:1:2:3::1 dPort 32
```

4.2.2.23 permit | deny(ipv6 standard)

Command:[no]{deny|permit}{{<*sIPv6Prefix*/*sPrefixlen*>} | any-source | {host-source <*sIPv6Addr*>}}

Function: Create a standard nomenclature IPv6 access control rule; the “no” form of this command deletes the nomenclature standard IPv6 access control rule.

Parameter:*<sIPv6Prefix>* is the prefix of the source IPv6 address,***<sPrefixlen>*** is the length of the IPv6 address prefix, the valid range is 1～128. ***<sIPv6Addr>*** is the source IPv6 address.

Command Mode: Standard IPv6 nomenclature access list mode

Default: No access list configured by default.

Usage Guide:

Example: Permit packets with source address of 2001:1:2:3::1/64 while denying those with source address of 2001:1:2:3::1/48.

```
Switch(config)# ipv6 access-list standard ipv6Flow
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# permit 2001:1:2:3::1/64
Switch(Config-IPv6-Std-Nacl-ipv6Flow)# deny 2001:1:2:3::1/48
```

4.2.2.24 time-range

Command:[no] time-range <*time_range_name*>

Functions: Create the name of time-range as time range name, enter the time-range mode at the same time.

Parameters:*time_range_name*,time range name must start with letter, and the length cannot exceed 16-character long.

Command Mode: Global mode

Default: No time-range configuration

Guide:

Examples: Reate a time-range named test.

```
Switch(config)#time-range test
```

4.3 ACL Example

Scenario:

The user has the following configuration requirement: port 1/10 of the switch connects to 10.0.0.0/24 segment, ftp is not desired for the user.

Configuration description:

a) Create a proper ACL
b) Configuring packet filtering function
c) Bind the ACL to the port

The configuration steps are listed below:

```
Switch(config)#access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch(config)#firewall enable
Switch(config)#firewall default permit
Switch(config)#interface ethernet1/10

Switch(Config-If-Ethernet1/10)#ip access-group 110 in
Switch(Config-If-Ethernet1/10)#exit
Switch(config)#exit
```

Configuration result.:

```
Switch#show firewall

Fire wall is enabled.
Firewall default rule is to permit any ip packet.
Switch#show access-lists
```

```
access-list 110(used 1 time(s))
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet1/10

interface name:Ethernet1/10
the ingress acl use in firewall is 110, traffic-statistics Disable.
```

4.4 ACL Troubleshooting

- Checking for entries in the ACL is done in a top-down order and ends whenever an entry is matched.
- Default rule will be used only if no ACL is bound to the incoming direction of the port, or no ACL entry is matched.
- Applies to IP packets incoming on all ports, and has no effect on other types of packets.
- One port can bound to only one incoming ACL.
- The number of ACLs that can be successfully bound depends on the content of the ACL bound and the hardware resource limit. Users will be prompted if an ACL cannot be bound due to hardware resource limitation.
- If an access-list contains same filtering information but conflicting action rules, binding to the port will fail with an error message. For instance, configuring "permit tcp any any-destination" and "deny tcp any any-destination" at the same time is not permitted.
- Viruses such as "worm.blaster" can be blocked by configuring ACL to block specific ICMP packets or specific TCP or UDP port packet.

4.4.1 Monitor And Debug Command

4.4.1.1 show access-lists

Command: show access-lists [<*num*>|<*acl-name*>]

Functions: Reveal ACL of configuration

Parameters: ***<acl-name>***, specific ACL name character string; ***<num>,*** specific ACL No.

Default: None

Command Mode: Admin mode

Usage Guide: When not assigning names of ACL, all ACL will be revealed, used x time（s）indicates the times of ACL to be used.

Examples:

```
Switch#show access-lists
access-list 10(used 0 time(s))
```

```
access-list 10 deny any
access-list 100(used 1 time(s))
access-list 100 deny ip any any-destination
access-list 100 deny tcp any any-destination
access-list 1100(used 0 time(s))
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800
access-list 3100(used 0 time(s))
access-list 3100 deny any-source-mac any-destination-mac udp any s-port 100 any-destination d-port 40000
```

Displayed information	Explanation
access-list 10(used 1 time(s))	Number ACL10, 0 time to be used
access-list 10 deny any	Deny any IP packets to pass
access-list 100(used 1 time(s))	Nnumber ACL10, 1 time to be used
access-list 100 deny ip any any-destination	Deny IP packet of any source IP address and destination address to pass
access-list 100 deny tcp any any-destination	Deny TCP packet of any source IP address and destination address to pass
access-list 1100 permit any-source-mac any-destination-mac tagged-eth2 14 2 0800	Permit tagged-eth2 with any source MAC addresses and any destination MAC addresses and the packets whose 15th and 16th byte is respectively 0x08 , 0x0 to pass
access-list 3100 permit any-source-mac any-destination-mac udp any s-port 100 any-destination d-port 40000	Deny the passage of UDP packets with any source MAC address and destination MAC address, any source IP address and destination IP address, and source port 100 and destination interface 40000

4.4.1.2 show access-group

Command: show access-group [interface [Ethernet] <*name*>]

Functions: Reveal tying situation of ACL on port

Parameters:<*name*>,Interface name

Default: None

Command Mode: Admin mode

Usage Guide: When not assigning interface names, all ACL tied to port will be revealed

Examples:

```
Switch#show access-group
```

```
interface name: Ethernet
the ingress acl use in firewall is 111,packet(s) number is 10.
the egress acl use in firewall is 100,packet(s) number is 10.
interface name: Ethernet
    the ingress acl use in firewall is 10,packet(s) number is 10.
```

Displayed information	Explanation
interface name: Ethernet	Tying situation on port Ethernet1/2
the ingress acl use in firewall is 111.	No. 111 numeric extended ACL tied to entrance of port Ethernet1/2
the egress acl use in firewall is 100.	No. 100 numeric extended ACL tied to entrance of port Ethernet1/2
interface name: Ethernet	Tying situation on port Ethernet1/2
the ingress acl use in firewall is 10.	No. 10 standard extended ACL tied to entrance of port Ethernet1/2
packet(s) number is 10	Number of packets matching this ACL rule

4.4.1.3 show firewall

Command: show firewall

Functions: Reveal configuration information of packet filtering functions

Parameters: None

Default: None

Command Mode: Admin mode

Examples:

```
Switch#show firewall
Fire wall is enabled.
Firewall default rule is to permit any ip packet.
```

Displayed information	Explanation
fire wall is enable	Packet filtering function enabled
the default action of firewall is permit	Default packet filtering function is permit

4.4.1.4 show time-range

Command: show time-range<*word*>

Functions: Reveal configuration information of time range functions

Parameters: ***word*** assign name of time-range needed to be revealed

Default: None

Command Mode: Admin mode

Usage Guide: When not assigning time-range names, all time-range will be revealed.

Examples:

```
Switch#show time-range
time-range timer1 (inactive)
absolute-periodic Saturday 0:0:0 to Sunday 23:59:59
time-range timer2 (active)
absolute-periodic Monday 0:0:0 to Friday 23:59:59
```

4.4.1.5 show ipv6 access-lists

Command: show ipv6 access-lists [<*num*>|<*acl-name*>]

Function: Show the configured IPv6 access control list

Parameter:<num> is the number of specific access control list, the valid range is 500～699,amongst 500～599 is digit standard IPv6 ACL number,600～699 is the digit extended IPv6 ACL number;<acl-name> is the nomenclature character string of a specific access control list, lengthening within 1～16.

Default: None

Command Mode: Admin Mode

Usage Guide: When no access control list is specified, all the access control lists will be displayed; in used x time（s） is shown the times the ACL had been quoted

Example:

```
Switch #show ipv6 access-lists
ipv6 access-list 500(used 1 time(s))
ipv6 access-list 500 deny any
ipv6 access-list 510(used 1 time(s))
ipv6 access-list 510 deny ip any any-destination
ipv6 access-list 510 deny tcp any any-destination
ipv6 access-list 520(used 1 time(s))
ipv6 access-list 520 permit ip any any-destination
```

4.5 Web Management

By clicking the ACL configuration icon, it will open up the ACL sub-sections which include the following parts:

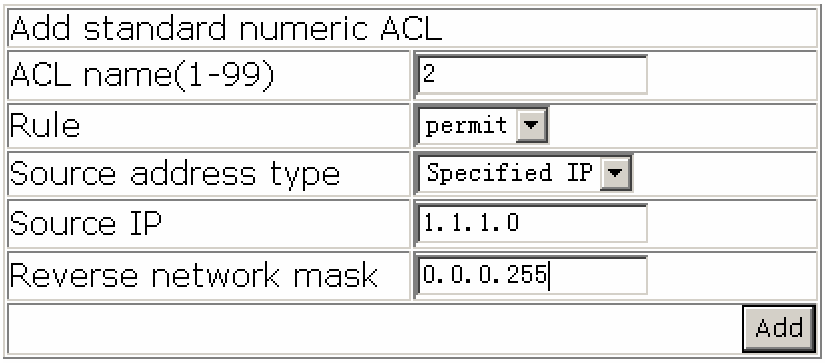
- Numeric ACL Configuration -Standard and Extended types
- ACL Name Configuration -Standard and Extended types
- Filter Configuration -- enable global configuration and the default action to bind ACL to the ports

4.5.1 Numeric standard ACL configuration

Click “Numeric ACL Configuration”, and then “Add Standard Numeric ACL” section to enter the configuration page. The explanations of each section are:

ACL number -1- 99
Rule -permit or deny
Source address type -Specified IP address or any randomly allocated IP address
Source IP address
Reverse network mask

Specify the number in the ACL number section and the relative values in the other 4 sections, then click “Add”, the users can then add the new Numeric Standard IP ACL.



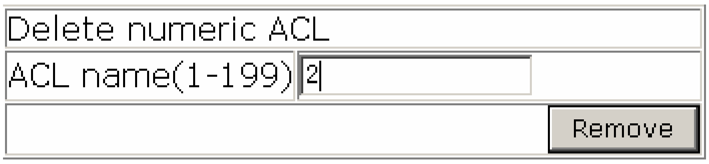
Add standard numeric ACL	
ACL name(1-99)	2
Rule	permit ▾
Source address type	Specified IP ▾
Source IP	1.1.1.0
Reverse network mask	0.0.0.255
	Add

4.5.2 Delete numeric IP ACL

Click “Numeric ACL Configuration”, and then “Delete Numeric ACL” section to enter the configuration page, The explanations of each section are:

ACL number (1-199)

To delete the Numeric ACL, just simply specify the number of ACL and then click the “Remove”.



Delete numeric ACL	
ACL name(1-199)	2
	Remove

4.5.3 Configure the numeric extended ACL

There are several extended numeric extended ACLs available:

- Add ICMP numeric extended ACL
- Add IGMP numeric extended ACL
- Add TCP numeric extended ACL
- Add UDP numeric extended ACL
- Add numeric extended ACL for other protocols

By clicking the icons, it will enter the related configuration page

There are several sub-sections in this category:

- ACL number (100-199)
- Rule - permit or deny
- Source address type - Specified IP address or any randomly allocated IP address
- Source IP address
- Reverse network mask
- Target address type - Specified IP address or any randomly allocated IP address
- Destination IP address
- Reverse network mask
- IP precedence
- TOS

Regarding “ICMP numeric extended ACL”, there are two sub-categories:

- ICMP type
- ICMP code

Regarding “IGMP numeric extended ACL”, there is one sub-category:

- IGMP type

Regarding “TCP numeric extended ACL”, there are three sub-categories:

- Source port
- Destination port
- TCP sign

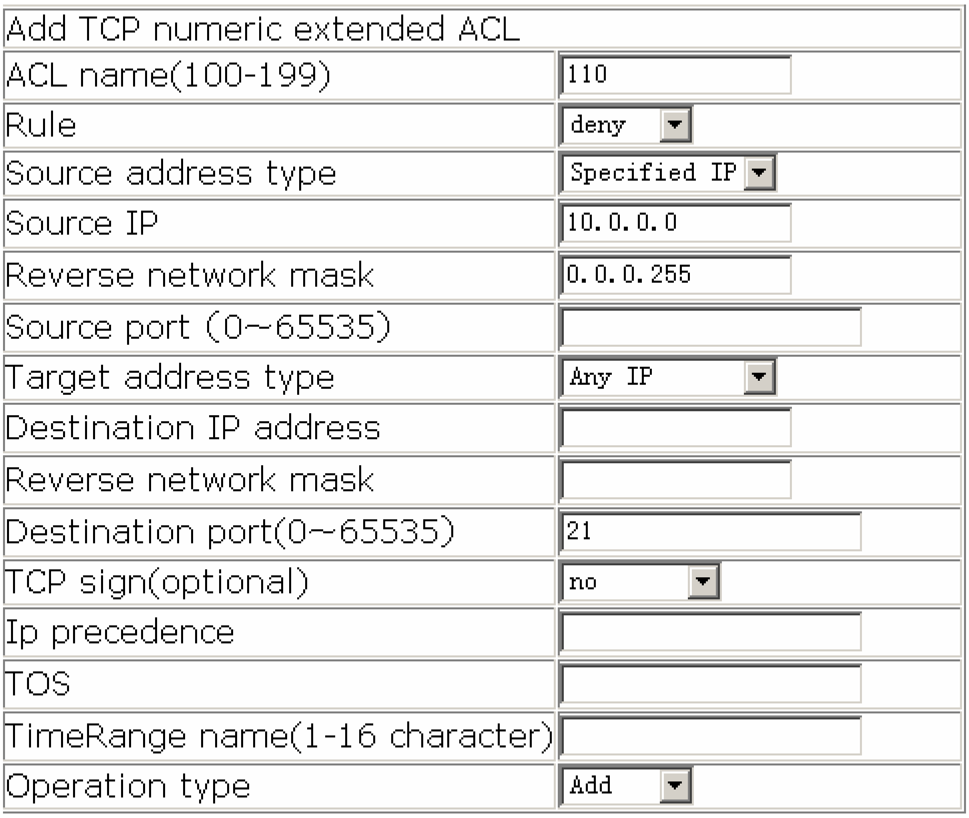
Regarding “UDP numeric extended ACL”, there are two sub-categories:

- Source port
- Target port

Regarding “numeric extended ACL for other protocols”, there is one sub-category: Matched protocol.

- Matched protocol - includes IP, EIGRP, OSPF, IPINIP and Input Protocol manually. If user selects to input manually, they can just simply key-in the protocol number in the right hand side of icon.

Example: a user wants to configure the “ Add TCP numeric extended ACL” with the ACL number of 110, deny the source IP address of 10.0.0.0/24 section, and make the target port is 21. Please refer the following configurations and then click the icon of “Add”.



Add TCP numeric extended ACL	
ACL name(100-199)	110
Rule	deny
Source address type	Specified IP
Source IP	10.0.0.0
Reverse network mask	0.0.0.255
Source port (0~65535)	
Target address type	Any IP
Destination IP address	
Reverse network mask	
Destination port(0~65535)	21
TCP sign(optional)	no
Ip precedence	
TOS	
TimeRange name(1-16 character)	
Operation type	Add

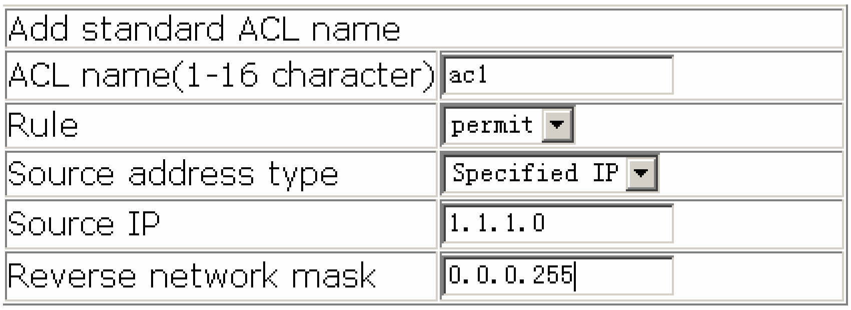
4.5.4 Configure and delete the standard ACL name

Click “ACL name configuration” to open up the sub-sections, next click “ACL name configuration” to enter the configuration page. The way to configure the “ACL name configuration” is the same with “Numeric ACL Configuration”. The only difference users should change the ACL number to the ACL name. This should be entered in ACL name not ACL number. CLI command: 1.2.2.6

There are seven sub-sections of this:

- ACL name
- ACL type - standard and extended
- Rule - permit and deny
- Source address type - Specified IP address or any randomly allocated IP address Source IP address
- Reverse network mask
- Operation type -Add or Remove

To add a numeric ACL, specify the ACL name and related value, select the “add” in the Operation type and then click “Apply”.



Add standard ACL name	
ACL name(1-16 character)	acl
Rule	permit
Source address type	Specified IP
Source IP	1.1.1.0
Reverse network mask	0.0.0.255

4.5.5 Configure extended ACL name configuration

Click “ACL name configuration”, the configuration sections will then be shown. There are 6 types of extended ACL name configurations:

- IP extended ACL name configuration
- ICMP extended ACL name configuration
- IGMP extended ACL name configuration
- TCP extended ACL name configuration
- UDP extended ACL name configuration
- Other protocols extended ACL name configuration

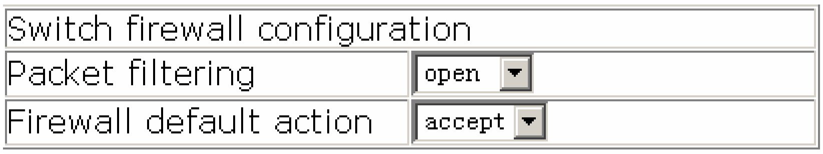
Click the related the configuration web page, the configuration is the same with it is with numeric extended ACL. The only difference is the ACL number needs to be changed to ACL name, and entered into the ACL name rather than number. CLI command: 1.2.2.5.

4.5.6 Firewall configuration

Click “Filter Configuration”, and then “Firewall Configuration” to enter the configuration page. The detailed explanation is as follows:

- Packet filtering -”open” to enable or “close” to disable.
- Firewall default action -”accept” means to allow the packet to pass through and “refuse” to deny the packet.

To enable or disable, users need to click “Apply” to confirm the command.



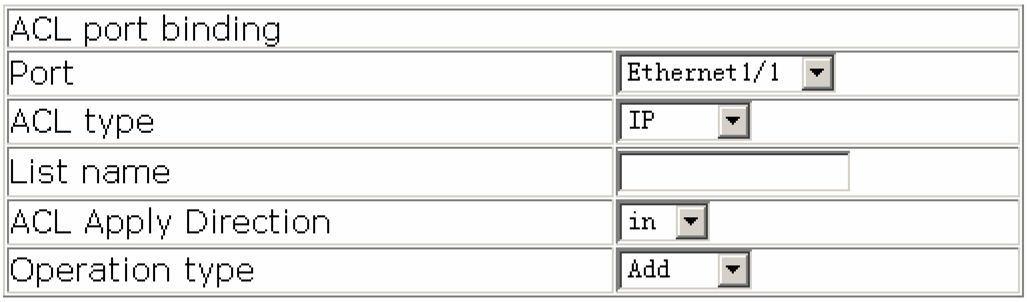
Switch firewall configuration	
Packet filtering	open
Firewall default action	accept

4.5.7 ACL port binding

Click “Filter configuration”, and then select “ACL port binding” to enter the configuration page. There are five items in this section.

- Port -the target port to bind to ACL
- ACL name -the target ACL name to bind
- Ingress/Egress -the target direction to bind
- Operation type -”Add” or “Remove”

To enable this function, you need to select the action in each item and then click “Apply”.



ACL port binding

Port	Ethernet1/1
ACL type	IP
List name	
ACL Apply Direction	in
Operation type	Add

Chapter 5 802.1x Configuration

5.1 Introduction to 802.1x

The 802.1x protocol originates from 802.11 protocol, the wireless LAN protocol of IEEE, which is designed to provide a solution to doing authentication when users access a wireless LAN. The LAN defined in IEEE 802 LAN protocol does not provide access authentication, which means as long as the users can access a LAN controlling device(such as a LAN Switch), they will be able to get all the devices or resources in the LAN. There was no looming danger in the environment of LAN in those primary enterprise networks.

However, along with the boom of applications like mobile office and service operating networks, the service providers should control and configure the access from user. The prevailing application of WLAN and LAN access in telecommunication networks, in particular, make it necessary to control ports in order to implement the user-level access control. And as a result, IEEE LAN/WAN committee defined a standard, which is 802.1x, to do Port-Based Network Access Control. This standard has been widely used in wireless LAN and ethernet.

"Port-Based Network Access Control" means to authenticate and control the user devices on the level of ports of LAN access devices. Only when the user devices connected to the ports pass the authentication, can they access the resources in the LAN, otherwise, the resources in the LAN won't be available.

5.1.1 The Authentication Structure of 802.1x

The system using 802.1x has a typical Client/Server structure, which contains three entities(as illustrated in the next figure): Supplicant system, Authenticator system, and Authentication server system.

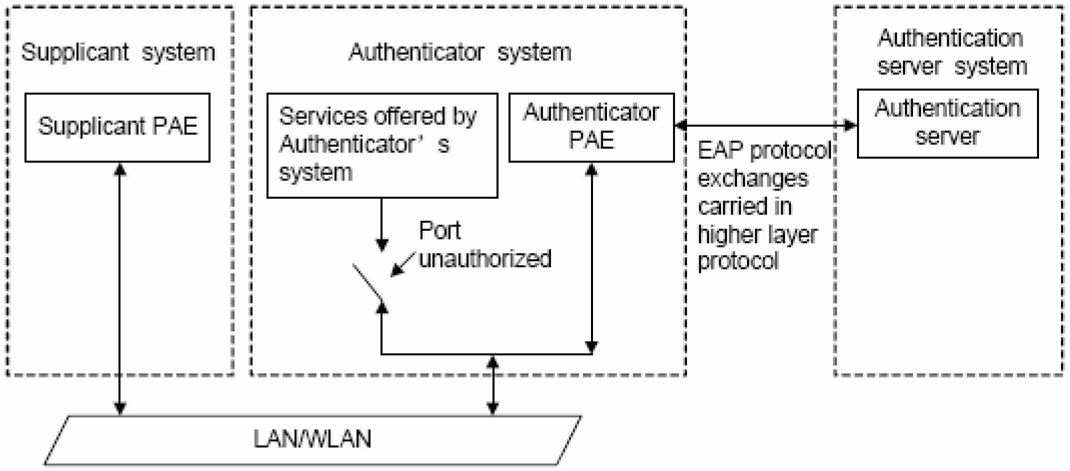

Supplicant system
Supplicant PAE
Authenticator system
Services offered by Authenticator' s system
Authenticator PAE
Port unauthorized
EAP protocol exchanges carried in higher layer protocol
Authentication server system
Authentication server
LAN/WLAN

Fig 5-1 The Authentication Structure of 802.1x

- ☞ The supplicant system is an entity on one end of the lan segment, should be authenticated by the access controlling unit on the other end of the link. A Supplicant system usually is a user terminal device. Users starts 802.1x authentication by starting supplicant system software. A supplicant system should support EAPOL(Extensible Authentication Protocol over LAN).
- ☞ The authenticator system is another entity on one end of the lan segment to authenticate the supplicant systems connected. An authenticator system usually is a network device supporting 802,1x protocol, providing ports to access the lan for supplicant systems. The ports provided can either be physical or logical.
- ☞ The authentication server system is an entity to provide authentication service for authenticator systems. The authentication server system is used to authenticate and authorize users, as well as do fee-counting, and usually is a RADIUS (Remote Authentication Dial-In User Service) server, which can store the relative user information, including username, password and other parameters such as the VLAN and ports which the user belongs to.

The three entities above concerns the following basic concepts: PAE of the port, the controlled ports and the controlled direction.

1. PAE

PAE (Port Access Entity) is the entity to implement the operation of algorithms and protocols.

- ☞ The PAE of the supplicant system is supposed to respond the authentication request from the authenticator systems and submit user’s authentication information to the authenticator system. It can also send authentication request and off-line request to authenticator.
- ☞ The PAE of the authenticator system authenticates the supplicant systems needing to access the LAN via the authentication server system, and deal with the authenticated/unauthenticated state of the controlled port according to the result of the authentication. The authenticated state means the user is allowed to access the network resources, the unauthenticated state means only the EAPOL messages are allowed to be received and sent while the user is forbidden to access network resources.

2. controlled/uncontrolled ports

The authenticator system provides ports to access the LAN for the supplicant systems. These ports can be divided into two kinds of logical ports: controlled ports and uncontrolled ports.-

- ☞ The uncontrolled port is always in bi-directionally connected status, and mainly used to transmit EAPOL protocol frames, to guarantee that the supplicant systems can always send or receive authentication messages.
- ☞ The controlled port is in connected status authenticated to transmit service messages. When unauthenticated, no message from supplicant systems is allowed to be received.
- ☞ The controlled and uncontrolled ports are two parts of one port, which means each frame reaching this port is visible on both the controlled and uncontrolled ports.

3. Controlled direction

In unauthenticated status, controlled ports can be set as unidirectionally controlled or bi-directionally controlled.

- ☞ When the port is bi-directionally controlled, the sending and receiving of all frames is forbidden.
- ☞ When the port is unidirectionally controlled, no frames can be received from the supplicant systems while sending frames to the supplicant systems is allowed.

Notes: At present, this kind of switch only supports unidirectional control.

5.1.2 The Work Mechanism of 802.1x

IEEE 802.1x authentication system uses EAP (Extensible Authentication Protocol) to implement exchange of authentication information between the supplicant system, authenticator system and authentication server system.

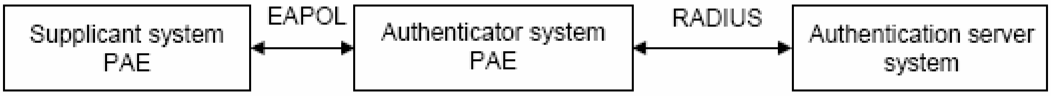


Fig 5-2 the Work Mechanism of 802.1x

- ☞ EAP messages adopt EAPOL encapsulation format between the PAE of the supplicant system and the PAE of the authenticator system in the environment of LAN.
- ☞ Between the PAE of the authenticator system and the RADIUS server, there are two methods to exchange information: one method is that EAP messages adopt EAPOR (EAP over RADIUS) encapsulation format in RADIUS protocol; the other is that EAP messages terminate with the PAE of the authenticator system, and adopt the messages containing RAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) attributes to do the authentication interaction with the RADIUS server.

- When the user pass the authentication, the authentication server system will send the relative information of the user to authenticator system, the PAE of the authenticator system will decide the authenticated/unauthenticated status of the controlled port according to the authentication result of the RADIUS server.

5.1.3 The Encapsulation of EAPOL Messages

1. The Format of EAPOL Data Packets

EAPOL is a kind of message encapsulation format defined in 802.1x protocol, and is mainly used to transmit EAP messages between the supplicant system and the authenticator system in order to allow the transmission of EAP messages through the LAN. In IEEE 802/Ethernet LAN environment, the format of EAPOL packet is illustrated in the next figure. The beginning of the EAPOL packet is the Type/Length domain in MAC frames.

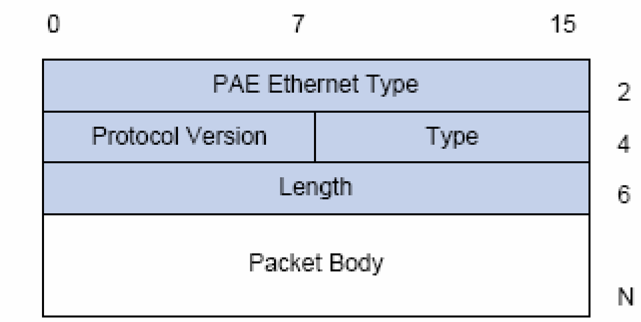


Fig 5-3 the Format of EAPOL Data Packet

PAE Ethernet Type: Represents the type of the protocol whose value is 0x888E.

Protocol Version: Represents the version of the protocol supported by the sender of EAPOL data packets.

Type: represents the type of the EAPOL data packets, including:

- EAP-Packet (whose value is 0x00): the authentication information frame, used to carry EAP messages. This kind of frame can pass through the authenticator system to transmit EAP messages between the supplicant system and the authentication server system.
- EAPOL-Start (whose value is 0x01): the frame to start authentication.
- EAPOL-Logoff (whose value is 0x02): the frame requesting to quit.
- EAPOL-Key (whose value is 0x03): the key information frame.
- EAPOL-Encapsulated-ASF-Alert (whose value is 0x04): used to support the Alerting messages of ASF (Alert Standard Forum). This kind of frame is used to encapsulate the relative information of network management such as all kinds of alerting information, terminated by terminal devices.

Length: represents the length of the data, that is, the length of the “Packet Body”, in byte. There will be no following data domain when its value is 0.

Packet Body: represents the content of the data, which will be in different formats according to different types.

2. The Format of EAP Data Packets

When the value of Type domain in EAPOL packet is EAP-Packet, the Packet Body is in EAP format (illustrated in the next figure).

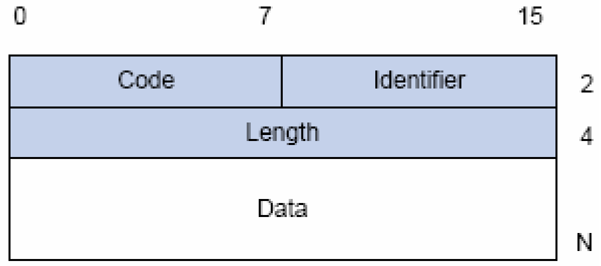


Fig 5-4 the Format of EAP Data Packets

Code: specifies the type of the EAP packet. There are four of them in total: Request（1）,Response（2）,Success（3）,Failure（4）.

☞ There is no Data domain in the packets of which the type is Success or Failure, and the value of the Length domains in such packets is 4.

☞ The format of Data domains in the packets of which the type is Request and Response is illustrated in the next figure. Type is the authentication type of EAP, the content of Type data depends on the type. For example, when the value of the type is 1, it means Identity, and is used to query the identity of the other side. When the type is 4, it means MD5-Challenge, like PPP CHAP protocol, contains query messages.

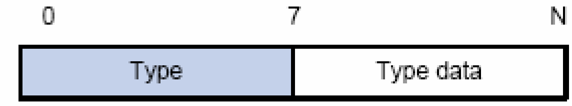


Fig 5-5 the Format of Data Domain in Request and Response Packets

Identifier: to assist matching the Request and Response messages.

Length: the length of the EAP packet, covering the domains of Code, Identifier, Length and Data, in byte.

Data: the content of the EAP packet, depending on the Code type.

5.1.4 The Encapsulation of EAP Attributes

RADIUS adds two attribute to support EAP authentication: EAP-Message and Message-Authenticator. Please refer to the Introduction of RADIUS protocol in “AAA-RADIUS-HWTACACS operation” to check the format of RADIUS messages.

1. EAP-Message

As illustrated in the next figure, this attribute is used to encapsulate EAP packet, the type code is 79, String domain should be no longer than 253 bytes. If the data length in an EAP packet is larger than 253 bytes, the packet can be divided into fragments, which then will be encapsulated in several EAP-Messages attributes in their original order.

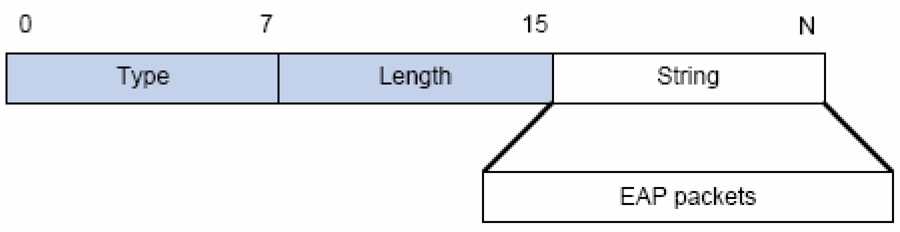


Fig 5-6 the Encapsulation of EAP-Message Attribute

2. Message-Authenticator

As illustrated in the next figure, this attribute is used in the process of using authentication methods like EAP and CHAP to prevent the access request packets from being eavesdropped. Message-Authenticator should be included in the packets containing the EAP-Message attribute, or the packet will be dropped as an invalid one.

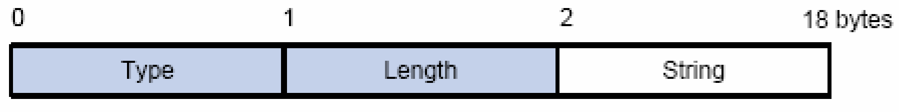


Fig 5-7 Message-Authenticator Attribute

5.1.5 Web Authentication Proxy based on 802.1x

The perspective of prior 802.1x authentication system abided by IEEE 802.1x authentication systems on architecture, working mechanism, business processes. The client authentication pattern of prior authentication system privately. The devices are layer 2 switch and the authentication server is RADIUS server. EAP protocol is used for the authentication message pattern. EAPOL encapsulation is used between client and the authentication proxy switch, that is to say, EAP message is encapsulated in the Ethernet frame to authenticate and communicate, however, EAPOR encapsulation is used between authentication proxy switch and authentication server, that is to say, EAP message is loaded on the Radius protocol to authenticate and communicate. it can be also forward by the device, transmit the PAP protocol message or CHAP protocol message based on the RADIUS protocol between the device and the RADIUS sever.

In 802.1x authentication system, in order to implement the identity authentication and the network permission, user should install the authentication client software, pass client login authentication progress and then achieve authenticated communication with RADIUS server. But some customers do not want to install client software, and they hope to authenticate by the internet explorer simplified. So in order to satisfy the new demand from the user and realize the platforms irrelevance of the authentication client, the Web authentication function based on 802.1x is designed for authentication.

The Web authentication is still based on IEEE 802.1x authentication system, the Java Applet in internet explorer is instead of the prior client software, the devises is layer 3 switch, authentication server is the standardized RADIUS server, and the authentication message is loaded in the EAP message to communicate. The Ethernet frame can't be send because of the Java Applet used in client, so EAP message can't be encapsulated in the Ethernet frame to send, EAP message should be loaded on the UDP protocol instead of EAPOU, in order to achieve the authentication and communication between web client and web authentication proxy switch. The standardized EAPOR protocol is still used between the authentication proxy switch and authentication server.

5.1.6 DHCP Option82 Based Dot1x Authorization

The number 82 of DHCP Relay Agent Information Option is implemented in order to support authentication based on dot1x protocol. In this mode, the switch will add respective option82 information in the DHCP request messages according to the authentication state of the client. When the DHCP server receives the DHCP request, it will allocate respective IP addresses according to the option82 information. Also, ACL can be configured on the trunk switches in order to control the access permission of the client.

5.1.7 The Authentication Methods of 802.1x

The authentication can either be started by supplicant system initiatively or by devices. When the device detects unauthenticated users to access the network, it will send supplicant system EAP-Request/Identity messages to start authentication. On the other hand, the supplicant system can send EAPOL-Start message to the device via supplicant software.

802.1x system supports EAP relay method and EAP termination method to implement authentication with the remote RADIUS server. The following is the description of the process of these two authentication methods, both started by the supplicant system.

5.1.7.1 EAP Relay Mode

EAP relay is specified in IEEE 802.1x standard to carry EAP in other high-level protocols, such as EAP over RADIUS, making sure that extended authentication protocol messages can reach the authentication server through complicated networks. In general, EAP relay requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator.

EAP is a widely-used authentication frame to transmit the actual authentication protocol rather than a special authentication mechanism. EAP provides some common function and allows the authentication mechanisms expected in the negotiation, which are called EAP Method. The advantage of EAP lies in that EAP mechanism working as a base needs no adjustment when a new authentication protocol appears. The following figure illustrates the protocol stack of

EAP authentication method.

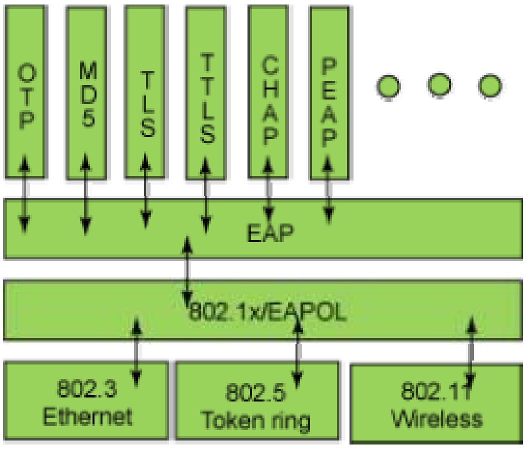


Fig 5-8 the Protocol Stack of EAP Authentication Method

By now, there are more than 50 EAP authentication methods has been developed, the differences among which are those in the authentication mechanism and the management of keys. The 4 most common EAP authentication methods are listed as follows:

- **EAP-MD5**
- **EAP-TLS**（Transport Layer Security）
- **EAP-TTLS**（Tunneled Transport Layer Security）
- **PEAP**（Protected Extensible Authentication Protocol）

- **EAP-MD5**
- **EAP-TLS**（Transport Layer Security）
- **EAP-TTLS**（Tunneled Transport Layer Security）
- **PEAP**（Protected Extensible Authentication Protocol）

They will be described in detail in the following part.

Attention：

- The switch, as the access controlling unit of Pass-through, will not check the content of a particular EAP method, so can support all the EAP methods above and all the EAP authentication methods that may be extended in the future.
- In EAP relay, if any authentication method in EAP-MD5, EAP-TLS, EAP-TTLS and PEAP is adopted, the authentication methods of the supplicant system and the RADIUS server should be the same.

1. EAP-MD5 Authentication Method

EAP-MD5 is an IETF open standard which providing the least security, since MD5 Hash function is vulnerable to dictionary attacks.

The following figure illustrated the basic operation flow of the EAP-MD5 authentication method.

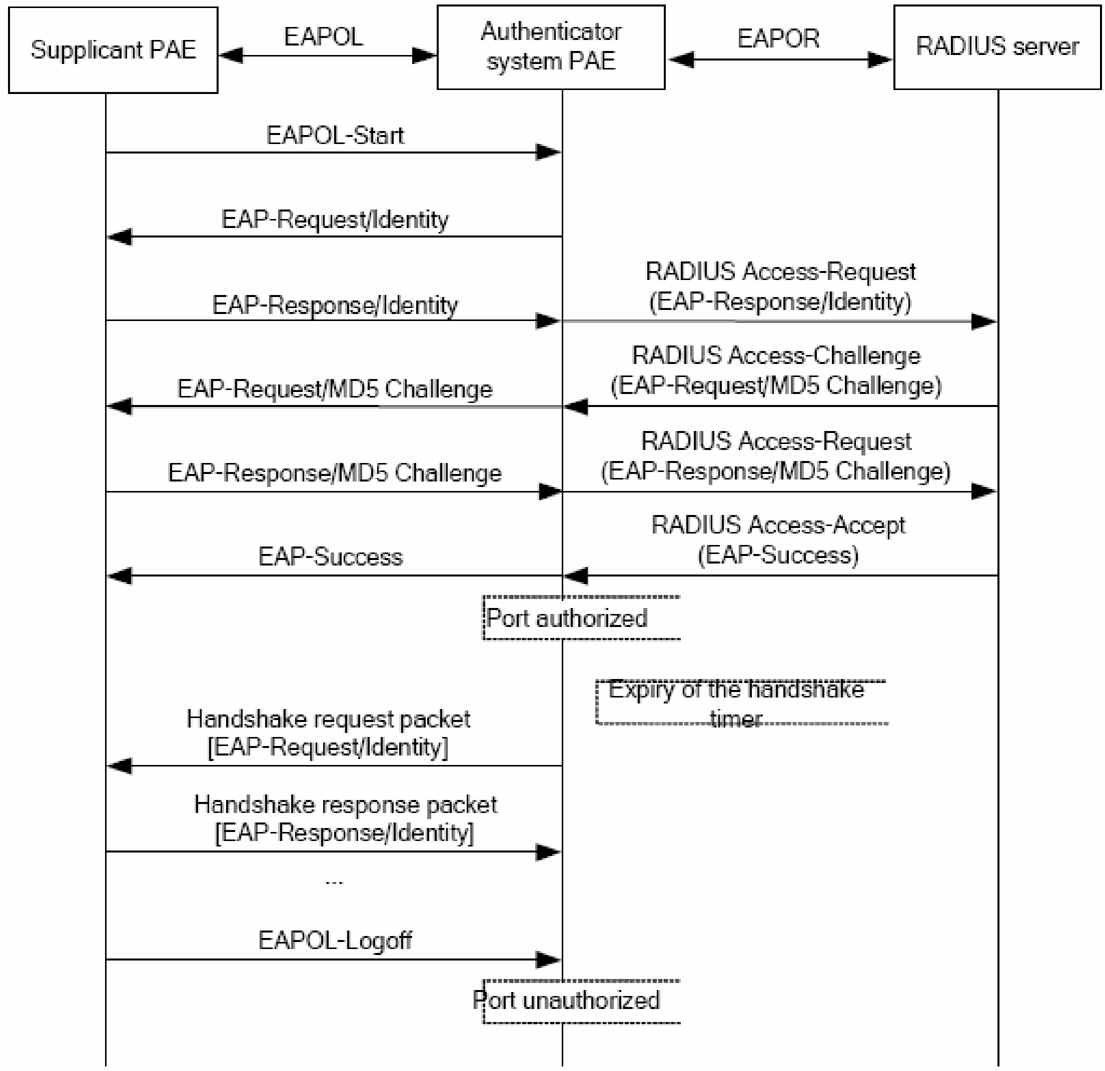

Supplicant PAE
EAPOL
Authenticator system PAE
EAPOR
RADIUS server
EAPOL-Start
EAP-Request/Identity
RADIUS Access-Request (EAP-Response/Identity)
EAP-Response/Identity
RADIUS Access-Challenge (EAP-Request/MD5 Challenge)
EAP-Request/MD5 Challenge
RADIUS Access-Request (EAP-Response/MD5 Challenge)
EAP-Response/MD5 Challenge
RADIUS Access-Accept (EAP-Success)
EAP-Success
Port authorized
Expiry of the handshake timer
Handshake request packet [EAP-Request/Identity]
Handshake response packet [EAP-Response/Identity]
...
EAPOL-Logoff
Port unauthorized

Fig 5-9 the Authentication Flow of 802.1x EAP-MD5

2. EAP-TLS Authentication Method

EAP-TLS is brought up by Microsoft based on EAP and TLS protocols. It uses PKI to protect the id authentication between the supplicant system and the RADIUS server and the dynamically generated session keys, requiring both the supplicant system and the Radius authentication server to possess digital certificate to implement bidirectional authentication. It is the earliest EAP authentication method used in wireless LAN. Since every user should have a digital certificate, this method is rarely used practically considering the difficult maintenance. However it is still one of the safest EAP standards, and enjoys prevailing supports from the vendors of wireless LAN hardware and software.

The following figure illustrates the basic operation flow of the EAP-TLS authentication method.

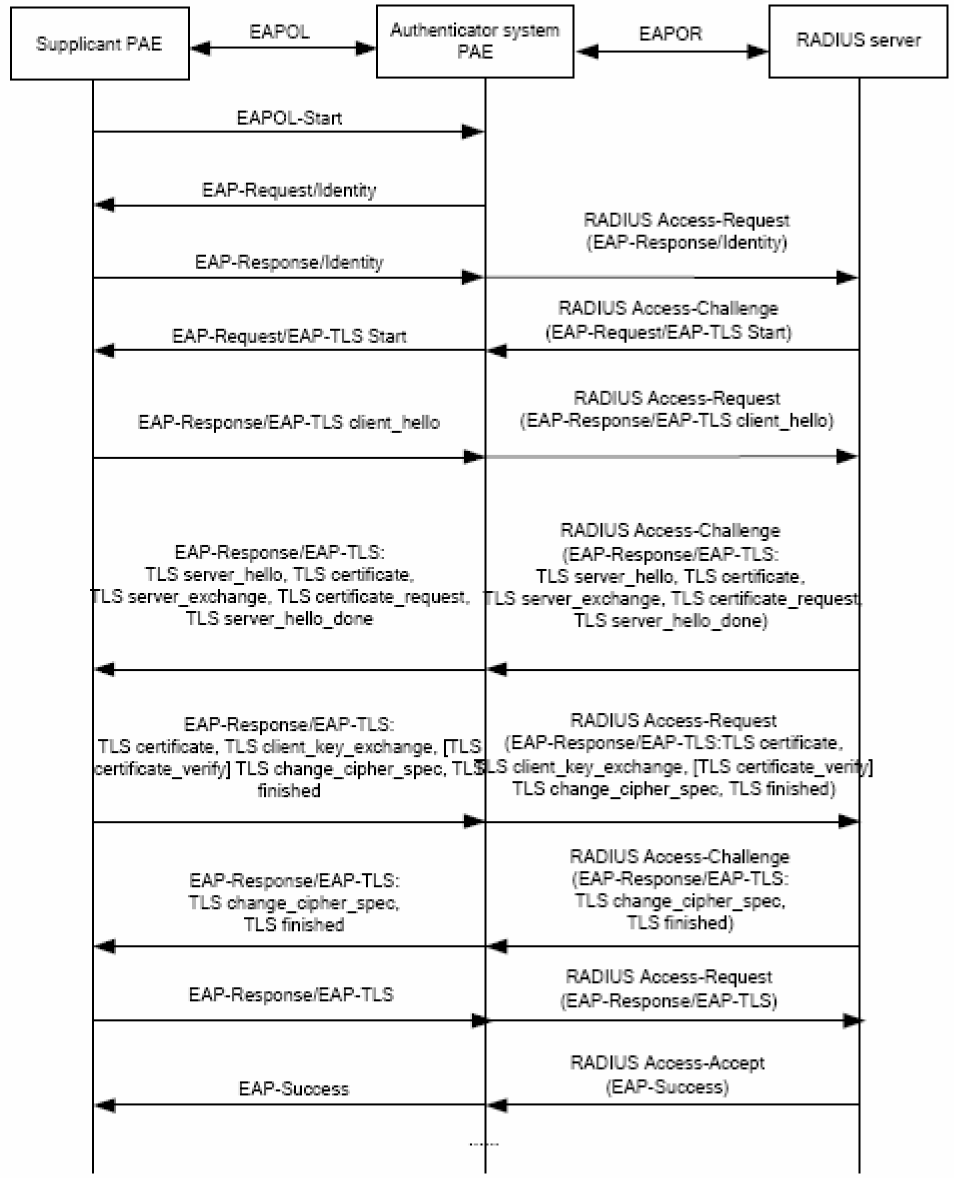

Supplicant PAE
EAPOL
Authenticator system PAE
EAPOR
RADIUS server
EAPOL-Start
EAP-Request/Identity
RADIUS Access-Request (EAP-Response/Identity)
EAP-Response/Identity
RADIUS Access-Challenge (EAP-Request/EAP-TLS Start)
EAP-Request/EAP-TLS Start
RADIUS Access-Request (EAP-Response/EAP-TLS client_hello)
EAP-Response/EAP-TLS client_hello
RADIUS Access-Challenge (EAP-Response/EAP-TLS: TLS server_hello, TLS certificate, TLS server_exchange, TLS certificate_request, TLS server_hello_done)
EAP-Response/EAP-TLS: TLS server_hello, TLS certificate, TLS server_exchange, TLS certificate_request, TLS server_hello_done
EAP-Response/EAP-TLS: TLS certificate, TLS client_key_exchange, [TLS certificate_verify] TLS change_cipher_spec, TLS finished
RADIUS Access-Request (EAP-Response/EAP-TLS:TLS certificate, TLS client_key_exchange, [TLS certificate_verify] TLS change_cipher_spec, TLS finished)
EAP-Response/EAP-TLS: TLS change_cipher_spec, TLS finished
RADIUS Access-Challenge (EAP-Response/EAP-TLS: TLS change_cipher_spec, TLS finished)
EAP-Response/EAP-TLS
RADIUS Access-Request (EAP-Response/EAP-TLS)
EAP-Success
RADIUS Access-Accept (EAP-Success)
......

Fig 5-10 the Authentication Flow of 802.1x EAP-TLS

3. EAP-TTLS Authentication Method

EAP-TTLS is a product of the cooperation of Funk Software and Certicom. It can provide an authentication as strong as that provided by EAP-TLS, but without requiring users to have their own digital certificate. The only request is that the Radius server should have a digital certificate. The authentication of users' identity is implemented with passwords transmitted in a safely encrypted tunnel established via the certificate of the authentication server. Any kind of authentication request including EAP, PAP and MS-CHAPV2 can be transmitted within TTLS tunnels.

4. PEAP Authentication Method

EAP-PEAP is brought up by Cisco, Microsoft and RAS Security as a recommended open standard. It has long been utilized in products and provides very good security. Its design of protocol and security is similar to that of EAP-TTLS, using a server's PKI certificate to establish a safe TLS tunnel in order to protect user authentication.

The following figure illustrates the basic operation flow of PEAP authentication method.

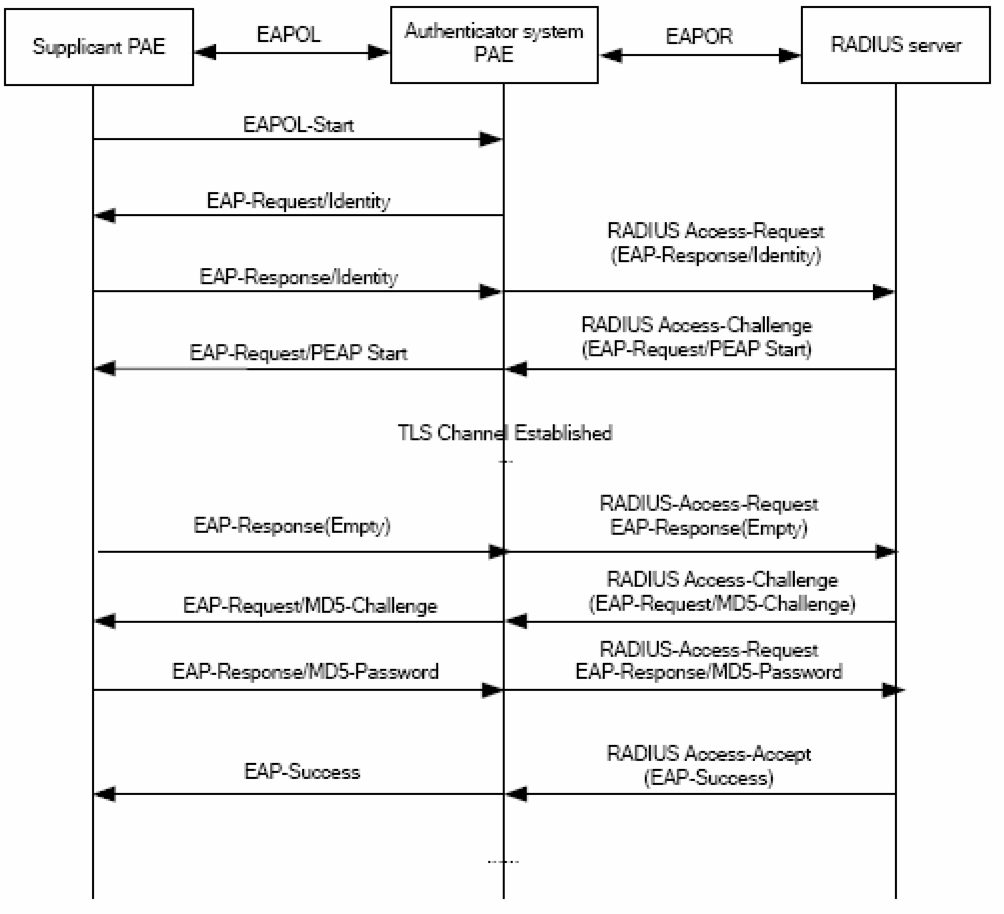
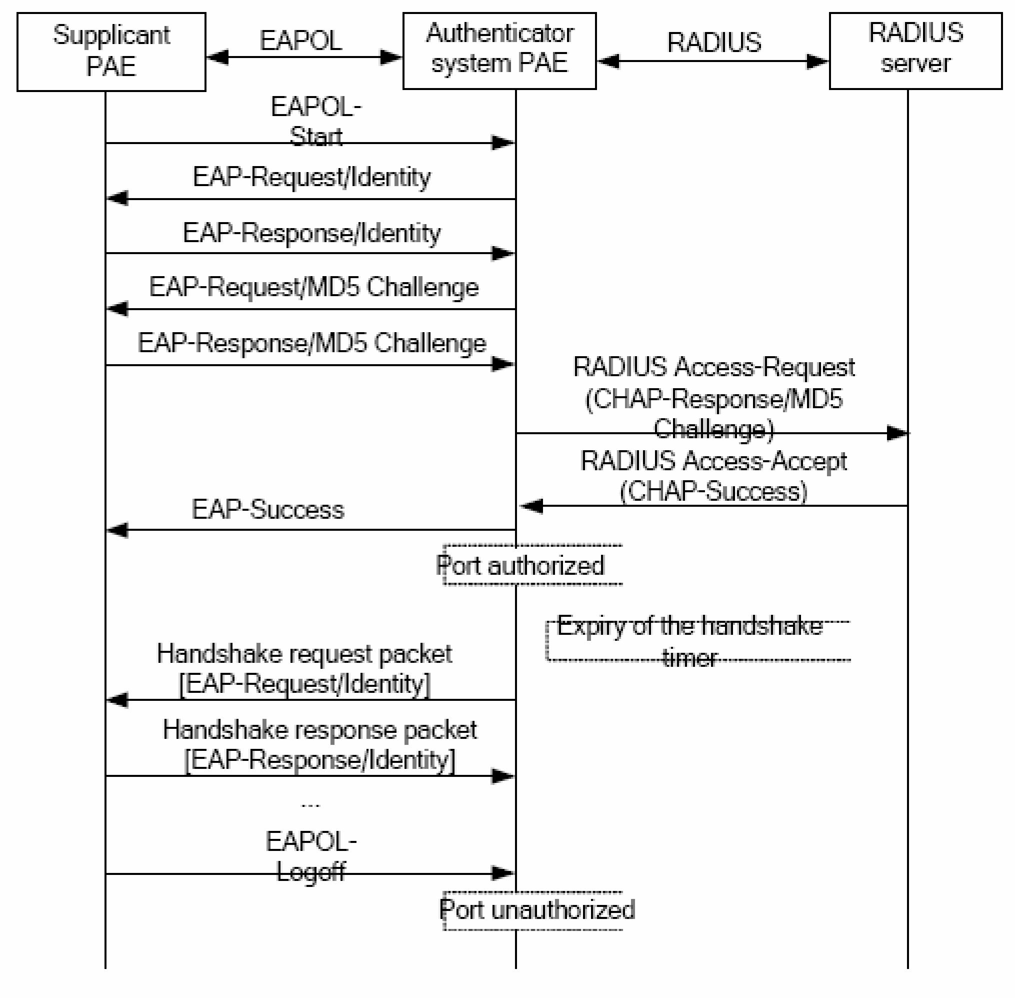

Supplicant PAE
EAPOL
Authenticator system PAE
EAPOR
RADIUS server
EAPOL-Start
EAP-Request/Identity
RADIUS Access-Request (EAP-Response/Identity)
EAP-Response/Identity
RADIUS Access-Challenge (EAP-Request/PEAP Start)
EAP-Request/PEAP Start
TLS Channel Established
RADIUS-Access-Request EAP-Response(Empty)
EAP-Response(Empty)
RADIUS Access-Challenge (EAP-Request/MD5-Challenge)
EAP-Request/MD5-Challenge
RADIUS-Access-Request EAP-Response/MD5-Password
EAP-Response/MD5-Password
RADIUS Access-Accept (EAP-Success)
EAP-Success

Fig 5-11 the Authentication Flow of 802.1x PEAP

5.1.7.2 EAP Termination Mode

In this mode, EAP messages will be terminated in the access control unit and mapped into RADIUS messages, which is used to implement the authentication, authorization and fee-counting. The basic operation flow is illustrated in the next figure.

In EAP termination mode, the access control unit and the RADIUS server can use PAP or CHAP authentication method. The following figure will demonstrate the basic operation flow using CHAP authentication method.



Supplicant PAE
EAPOL
Authenticator system PAE
RADIUS
RADIUS server
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
EAP-Request/MD5 Challenge
EAP-Response/MD5 Challenge
RADIUS Access-Request (CHAP-Response/MD5 Challenge)
RADIUS Access-Accept (CHAP-Success)
EAP-Success
Port authorized
Expiry of the handshake timer
Handshake request packet [EAP-Request/Identity]
Handshake response packet [EAP-Response/Identity]
...
EAPOL-Logoff
Port unauthorized

Fig 5-12 the Authentication Flow of 802.1x EAP Termination Mode

5.1.8 The Extension and Optimization of 802.1x

Besides supporting the port- based access authentication method specified by the protocol, devices also extend and optimize it when implementing the EAP relay mode and EAP termination mode of 802.1x.

- ☞ Supports some applications in the case of which one physical port can have more than one users
- ☞ There are three access control methods (the methods to authenticate users): port-based, MAC-based and user-based (IP address+ MAC address+ port).
  - ◆ When the port-based method is used, as long as the first user of this port passes the authentication, all the other users can access the network resources without being authenticated. However, once the first user is offline, the network won’t be available to all the other users.
  - ◆ When the MAC-based method is used, all the users accessing a port should be authenticated separately, only those pass the authentication can access the

network, while the others can not. When one user becomes offline, the other users will not be affected.

- When the user-based (IP address+ MAC address+ port) method is used, all users can access limited resources before being authenticated. There are two kinds of control in this method: standard control and advanced control. The user-based standard control will not restrict the access to limited resources, which means all users of this port can access limited resources before being authenticated. The user-based advanced control will restrict the access to limited resources, only some particular users of the port can access limited resources before being authenticated. Once those users pass the authentication, they can access all resources.

Attention: when using private supplicant systems, user-based advanced control is recommended to effectively prevent ARP cheat.

The maximum number of the authenticated users can be 4000, but less than 2000 will be preferred.

5.1.9 The Features of VLAN Allocation

1. Auto VLAN

Auto VLAN feature enables RADIUS server to change the VLAN to which the access port belongs, based on the user information and the user access device information. When an 802.1x user passes authentication on the server, the RADIUS server will send the authorization information to the device, if the RADIUS server has enabled the VLAN-assigning function, then the following attributes should be included in the Access-Accept messages:

- ☞ Tunnel-Type = VLAN (13)
- ☞ Tunnel-Medium-Type = 802 (6)
- ☞ Tunnel-Private-Group-ID = VLANID

The VLANID here means the VID of VLAN, ranging from 1 to 4094. For example, Tunnel-Private-Group-ID = 30 means VLAN 30.

When the switch receives the assigned Auto VLAN information, the current Access port will leave the VLAN set by the user and join Auto VLAN.

Auto VLAN won’t change or affect the port’s configuration. But the priority of Auto VLAN is higher than that of the user-set VLAN, that is Auto VLAN is the one takes effect when the authentication is finished, while the user-set VLAN do not work until the user become offline.

Notes: At present, Auto VLAN can only be used in the port-based access control mode, and on the ports whose link type is Access.

2. Guest VLAN

Guest VLAN feature is used to allow the unauthenticated user to access some specified resources.

The user authentication port belongs to a default VLAN (Guest VLAN) before passing the 802.1x authentication, with the right to access the resources within this VLAN without authentication. But the resources in other networks are beyond reach. Once authenticated, the port will leave Guest VLAN, and the user can access the resources of other networks.

In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications (such as anti-virus software, the patches of operating system). The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.

Once the 802.1x feature is enabled and the Guest VLAN is configured properly, a port will be added into Guest VLAN, just like Auto VLAN, if there is no response message from the supplicant system after the device sends more authentication-triggering messages than the upper limit (EAP-Request/Identity) from the port.

- ☞ The authentication server assigns an Auto VLAN, and then the port leaves Guest VLAN and joins the assigned Auto VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.
- ☞ The authentication server assigns an Auto VLAN, and then the port leaves Guest VLAN and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified Guest VLAN again.

5.2 802.1x Configuration

5.2.1 802.1x Configuration Task Sequence

1. Enable IEEE 802.1x function
2. Configure web authentication agent function
3. Access management unit property configuration

   1) Configure port authentication status

   2) Configure access management method for the port: MAC-based or port-based.

   3) Configure expanded 802.1x function

   4) Configure IPv6 pass through function

4. User access devices related property configuration (optional)

1. Enable 802.1x function

Command	Explanation
Global Mode	
dot1x enable **no dot1x enable**	Enables the 802.1x function in the switch and ports; the "**no dot1x enable**" command disables the 802.1x function.
dot1x user free-resource ***<prefix>*** ***<mask>*** **no dot1x user free-resource**	Sets free access network resource for unauthorized dot1x user. The "**no dot1x user free-resource**" command close the resource.

2. Configure Web authentication agent function

Command	**Explanation**
Global Mode	
dot1x web authentication enable **no dot1x web authentication enable**	Enable Web authentication agent, the "**no dot1x web authentication enable"** command disable Web authentication agent.
dot1x web redirect ***<URL>*** **no dot1x web redirect**	Set the HTTP server address for Web redirection, the **"no dot1x web redirect"** command clear the address.

3. Access management unit property configuration

1) Configure port authentication status

Command	**Explanation**
Port Mode	
dot1x port-control {auto|force-authorized|force-unauthorized } **no dot1x port-control**	Sets the 802.1x authentication mode; the "**no dot1x port-control**" command restores the default setting.

2) Configure port access management method

Command	Explanation
Port Mode	
dot1x port-method {macbased | portbased | webbased | userbased {standard|advanced} | dhcpoption82based } **no dot1x port-method**	Sets the port access management method; the "**no dot1x port-method**" command restores MAC-based access management.
dot1x max-user macbased <*number*> **no dot1x max-user macbased**	Sets the maximum number of access users for the specified port; the "**no dot1x max-user macbased**" command restores the default setting of allowing 1 user.
dot1x max-user userbased <*number*> **no dot1x max-user userbased**	Set the upper limit of the number of users allowed to access the specified port, only used when the access control mode of the port is userbased; the "**no dot1x max-user userbased**" command is used to reset the limit to 10 by default.
dot1x guest-vlan <*vlanID*> **no dot1x guest-vlan**	Set the guest vlan of the specified port; the "**no dot1x guest-vlan**" command is used to delete the guest vlan.

3) Configure expanded 802.1x function

Command	Explanation
Global Mode	
dot1x macfilter enable **no dot1x macfilter enable**	Enables the 802.1x address filter function in the switch; the "no dot1x macfilter enable" command disables the 802.1x address filter function.
dot1x accept-mac <mac-address> [interface <interface-name>] **no dot1x accept-mac <mac-address> [interface <interface-name>]**	Adds 802.1x address filter table entry, the "no dot1x accept-mac" command deletes 802.1x filter address table entries.
dot1x eapor enable **no dot1x eapor enable**	Enables the EAP relay authentication function in the switch; the "no dot1x eapor enable" command sets EAP local end authentication.

4) Configure IPv6 pass through function

Command	Explanation
Port Mode	
dot1x ipv6 passthrough **no dot1x ipv6 passthrough**	Enable IPv6 pass through function on a switch port, only applicable when access control mode is userbased; the no operation will disable the function.

4. Supplicant related property configuration

Command	Explanation
Global Mode	
dot1x max-req <count> **no dot1x max-req**	Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response, the "no dot1x max-req" command restores the default setting.
dot1x re-authentication **no dot1x re-authentication**	Enables periodical supplicant authentication; the "no dot1x re-authentication" command disables this function.
dot1x timeout quiet-period <seconds> **no dot1x timeout quiet-period**	Sets time to keep silent on port authentication failure; the "no dot1x timeout quiet-period" command restores the default value.
dot1x timeout re-authperiod <seconds> **no dot1x timeout re-authperiod**	Sets the supplicant re-authentication interval; the "no dot1x timeout re-authperiod" command restores the default setting.
dot1x timeout tx-period <seconds> **no dot1x timeout tx-period**	Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "no dot1x timeout tx-period" command restores the default setting.
dot1x re-authenticate [interface <interface-name>]	Enables IEEE 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

5.2.2 Command for 802.1x

5.2.2.1 dot1x accept-mac

Command: dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]

Function: Adds a MAC address entry to the dot1x address filter table. If a port is specified, the entry added applies to the specified port only. If no port is specified, the entry added applies to all the ports. The "**no dot1x accept-mac <*mac-address*> [interface <*interface-name*>]**" command deletes the entry from dot1x address filter table.

Parameters: <*mac-address*> stands for MAC address; **<*interface-name*>** for interface name and port number.

Command mode: Global Mode

Default: N/A.

Usage Guide: The dot1x address filter function is implemented according to the MAC address filter table, dot1x address filter table is manually added or deleted by the user. When a port is specified in adding a dot1x address filter table entry, that entry applies to the port only; when no port is specified, the entry applies to all ports in the switch. When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted, the rest will be rejected.

Example: Adding MAC address 00-01-34-34-2e-0a to the filter table of Ethernet 1/5.

```
Switch(config)#dot1x accept-mac 00-01-34-34-2e-0a interface ethernet 1/5
```

5.2.2.2 dot1x eapor enable

Command: dot1x eapor enable

no dot1x eapor enable

Function: Enables the EAP relay authentication function in the switch; the "**no dot1x eapor enable**" command sets EAP local end authentication.

Command mode: Global Mode

Default: EAP relay authentication is used by default.

Usage Guide: The switch and RADIUS may be connected via Ethernet or PPP. If an Ethernet connection exists between the switch and RADIUS server, the switch needs to authenticate the user by EAP relay (EAPoR authentication); if the switch connects to the RADIUS server by PPP, the switch will use EAP local end authentication (CHAP authentication). The switch should use different authentication methods according to the connection between the switch and the authentication server.

Example: Setting EAP local end authentication for the switch.

```
Switch(config)#no dot1x eapor enable
```

5.2.2.3 dot1x enable

Command: dot1x enable

no dot1x enable

Function: Enables the 802.1x function in the switch and ports: the "**no dot1x enable**" command disables the 802.1x function.

Command mode: Global Mode and Interface Mode.

Default: 802.1x function is not enabled in global mode by default; if 802.1x is enabled under Global Mode, 802.1x will not be enabled for the ports by default.

Usage Guide: The 802.1x authentication for the switch must be enabled first to enable 802.1x authentication for the respective ports. If Spanning Tree or MAC binding is enabled on the port, or the port is a Trunk port or member of port aggregation group, 802.1x function cannot be enabled for that port unless such conditions are removed.

Example: Enable the 802.1x function of the switch and enable 802.1x for port 1/12.

```
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/12
Switch(Config-If-Ethernet1/12)#dot1x enable
```

5.2.2.4 dot1x ipv6 passthrough

Command：dot1x ipv6 passthrough

no dot1x ipv6 passthrough

Function：Enable IPv6 pass through function on a switch port, only applicable when access control mode is userbased; the no operation of this command will disable the function.

Command Mode：Port Mode.

Default Settings：Pv6 pass through function is disabled on the switch by default.

Usage Guide：The function can only be enabled when 802.1x function is enabled both globally and on the port, with userbased being the control access mode. After it is enabled, users can send ipv6 messages without verification.

Examples：Enable IPv6 pass through function on port Ethernet1/12.

```
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/12
Switch(Config-If-Ethernet1/12)#dot1x enable
Switch(Config-If-Ethernet1/12)#dot1x ipv6 passthrough
```

5.2.2.5 dot1x guest-vlan

Command：dot1x guest-vlan <*vlanid*>

no dot1x guest-vlan

Function：Set the guest-vlan of the specified port; the “**no dot1x guest-vlan**” command is used to delete the guest-vlan.

Parameters：<*vlanid*> the specified Vlan id, ranging from 1 to 4094。

Command Mode：Interface Mode.

Default Settings：There is no 802.1x guest-vlan function on the port.

User Guide：The access device will add the port into Guest VLAN if there is no supplicant getting authenticated successfully in a certain stretch of time because of lacking exclusive authentication supplicant system or the version of the supplicant system being too low.

In Guest VLAN, users can get 802.1x supplicant system software, update supplicant system or update some other applications(such as anti-virus software, the patches of operating system). When a user of a port within Guest VLAN starts an authentication, the port will remain in Guest VLAN in the case of a failed authentication. If the authentication finishes successfully, there are two possible results:

☞ The authentication server assigns an Auto VLAN, causing the port to leave Guest VLAN to join the assigned Auto VLAN. After the user gets offline, the port will be allocated back into the specified Guest Vlan.

☞ The authentication server assigns an Auto VLAN, then the port leaves Guest VLAn and joins the specified VLAN. When the user becomes offline, the port will be allocated to the specified GuestVlan again.

Attention:

☞ There can be different Guest VLAN set on different ports, while only one Guest VLAN is allowed on one port.

☞ Only when the access control mode is portbased, the Guest VLAN can take effect. If the access control mode of the port is macbased or userbased, the Guest VLAN can be successfully set without taking effect.

Examples：Set Guest-Vlan of port Ethernet1/3 as Vlan 10.

Switch(Config-If-Ethernet1/3)#dot1xguest-vlan 10

5.2.2.6 dot1x macfilter enable

Command: dot1x macfilter enable

no dot1x macfilter enable

Function: Enables the dot1x address filter function in the switch; the "**no dot1x macfilter enable**" command disables the dot1x address filter function.

Command mode: Global Mode

Default: dot1x address filter is disabled by default.

Usage Guide: When dot1x address filter function is enabled, the switch will filter the authentication user by the MAC address. Only the authentication request initialed by the users in the dot1x address filter table will be accepted.

Example: Enable dot1x address filter function for the switch.

Switch(config)#dot1x macfilter enable

5.2.2.7 dot1x max-req

Command: dot1x max-req <*count*>

no dot1x max-req

Function: Sets the number of EAP request/MD5 frame to be sent before the switch re-initials authentication on no supplicant response; the "**no dot1x max-req**" command restores the default setting.

Parameters: <*count*> is the times to re-transfer EAP request/ MD5 frames, the valid range is 1 to 10.

Command mode: Global Mode

Default: The default maximum for retransmission is 2.

Usage Guide: The default value is recommended in setting the EAP request/ MD5 retransmission times.

Example: Changing the maximum retransmission times for EAP request/ MD5 frames to 5 times.

```
Switch(config)#dot1x max-req 5
```

5.2.2.8 dot1x user free-resource

Command：**dot1x user free-resource <*prefix*> <*mask*>**

no dot1x user free-resource

Function: Sets free access network resource for unauthorized dot1x user. The "no dot1x user free-resource" command close the resource.

Parameters:<*prefix*> is the resource IP network address in dotted decimal notation. **<*mask*>**is the subnet mask in dotted decimal notation.

Command mode: Globle Mode.

Default: no free resource set.

Usage guide: The command is used only for dot1x port-methods user-based access management. For dot1x port-methods userbased access management, the unauthorized user can access the free-resource set by the command. For dot1x port-methods port-based and MAC-based access management, none of resource is accessible for unauthorized user.

If TRUSTVIEW management system is available, the free resource can be configured in TRUSTVIEW server, and the TRUSTVIEW server will distribute the configuration to the switches.

note: can set only one resource IP network address.

Example: Sets the resource network address to be1.1.1.0，subnet mask to be 255.255.255.0.

```
Switch(config)#dot1x user free-resource 1.1.1.0 255.255.255.0
```

5.2.2.9 dot1x max-user macbased

Command: dot1x max-user macbased<*number*>

no dot1x max-user macbased

Function: Sets the maximum users allowed to connect to the port; the “**no dot1x max-user**” command restores the default setting.

Parameters: < *number*> is the maximum users allowed, the valid range is 1 to 256.

Command mode: Port configuration Mode.

Default: The default maximum user allowed is 1.

Usage Guide: This command is available for ports using MAC-based access management, if MAC address authenticated exceeds the number of allowed user, additional users will not be able to access the network.

Example: Setting port 1/3 to allow 5 users.

```
Switch(Config-If-Ethernet1/3)#dot1x max-user macbased 5
```

5.2.2.10 dot1x max-user userbased

Command：dot1x max-user userbased <*number*>
no dot1x max-user userbased

Function： Set the upper limit of the number of users allowed to access the specified port when using user-based access control mode; the “no dot1x max-user userbased” command is used to reset the default value .

Parameters：<*number*> the maximum number of users allowed to access the network, ranging from 1 to 1~256.

Command Mode： Interface Mode.

Default Settings： The maximum number of users allowed to access each port is 10 by default.

User Guide： This command can only take effect when the port adopts user-based access control mode. If the number of authenticated users exceeds the upper limit of the number of users allowed to access the network, those extra users can not access the network.

Examples： Setting port 1/3 to allow 5 users..

```
Switch(Config-If-Ethernet1/3)#dot1x max-user userbased 5
```

5.2.2.11 dot1x port-control

Command:dot1x port-control {auto|force-authorized|force-unauthorized }
no dot1x port-control

Function: Sets the 802.1x authentication status; the “**no dot1x port-control**” command restores the default setting.

Parameters:auto enable 802.1x authentication, the port authorization status is determined by the authentication information between the switch and the supplicant; **force-authorized** sets port to authorized status, unauthenticated data is allowed to pass through the port; **force-unauthorized** will set the port to non-authorized mode, the switch will not provide authentication for the supplicant and prohibit data from passing through the port.

Command mode: Port configuration Mode

Default: When 802.1x is enabled for the port, **auto** is set by default.

Usage Guide: If the port needs to provide 802.1x authentication for the user, the port authentication mode should be set to **auto**.

Example: Setting port1/1 to require 802.1x authentication mode.

Switch(config)#interface ethernet 1/1

Switch(Config-If-Ethernet1/1)#dot1x port-control auto

5.2.2.12 dot1x port-method

Command: dot1x port-method {macbased | portbased| webbased | userbased advanced | dhcpoption82based }

no dot1x port-method

Function: Sets the access management method for the specified port; the "**no dot1x port-method**" command restores the default access management method.

Parameters: macbased sets the MAC-based access management method; **portbased** sets port-based access management. **userbased** sets user-based access management, it includes two types of control, the standard and advanced. **Dhcpoption82based** means the access control method based on dhcp option82.

Command mode: Port configuration Mode

Default: None.

Usage Guide: For MAC-based access management, Multi-user is allowed to authenticate.For port-based access management only one user is allowed to authenticate.For both MAC-based and port-based access management, None of the network resource is available for unauthorized user.

For user-based standard access management, the special network resource is available for unauthorized user, all the network resource is available for authorized user. For user-based acvanced access management, the special network resource is available only for special unauthorized user, all the network resource is available for authorized user.

Webbased access management is used mostly in L3 switch.The global configuration of WEB authentication agent and HTTP redirection address is needed before setting the port to Webbased access management. Webbased access management is conflicted with the command of "ip dhcp snooping binding user-control".

For the DHCP option 82 based access control method, hosts with DHCP client software will get different IP addresses before and after the authentication, and both can access the network resources. In this mode, the DHCP allocates addresses according to the option 82 information. When hosts are trying to get IP address through DHCP, the switch will append specific option 82 information to the DHCP request according to the authentication state of the host. Then the DHCP server allocates addresses according to this information. At the same time, ACL can be configured in the trunk switch which is connected to the access switch, to control the network resources the host can access. Option 82 information is by default before authentication, while after authentication, the TRUSTVIEW system decides its content and deliver it to the switch.

Example: Setting port-based access management for port 1/4.

Switch(Config-If-Ethernet1/4)#dot1x port-method portbased

5.2.2.13 dot1x re-authenticate

Command: dot1x re-authenticate [interface <*interface-name*>]

Function: Enables real-time 802.1x re-authentication (no wait timeout requires) for all ports or a specified port.

Parameters: <*interface-nam*> stands for port number, omitting the parameter for all ports.

Command mode: Global Mode

Usage Guide: This command is an Global Mode command. It makes the switch to re-authenticate the client at once without waiting for re-authentication timer timeout. This command is no longer valid after authentication.

Example: Enable real-time re-authentication on port 1/8.

Switch(config)#dot1x re-authenticate interface ethernet 1/8

5.2.2.14 dot1x re-authentication

Command: dot1x re-authentication

no dot1x re-authentication

Function: Enables periodical supplicant authentication; the "**no dot1x re-authentication**" command disables this function.

Command mode: Global Mode

Default: Periodical re-authentication is disabled by default.

Usage Guide: When periodical re-authentication for supplicant is enabled, the switch will re-authenticate the supplicant at regular interval. This function is not recommended for common use.

Example: Enable the periodical re-authentication for authenticated users.

Switch(config)#dot1x re-authentication

5.2.2.15 dot1x timeout quiet-period

Command: dot1x timeout quiet-period <*seconds*>

no dot1x timeout quiet-period

Function: Sets time to keep silent on supplicant authentication failure; the "**no dot1x timeout quiet-period**" command restores the default value.

Parameters: <*seconds*> is the silent time for the port in seconds, the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 10 seconds.

Usage Guide: Default value is recommended.

Example: Setting the silent time to 120 seconds.

```
Switch(config)#dot1x timeout quiet-period 120
```

5.2.2.16 dot1x timeout re-authperiod

Command: dot1x timeout re-authperiod <*seconds*>

no dot1x timeout re-authperiod

Function: Sets the supplicant re-authentication interval; the "**no dot1x timeout re-authperiod**" command restores the default setting.

Parameters: <*seconds*> is the interval for re-authentication, in seconds, the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 3600 seconds.

Usage Guide: dot1x re-authentication must be enabled first before supplicant re-authentication interval can be modified. If authentication is not enabled for the switch, the supplicant re-authentication interval set will not take effect.

Example: Setting the re-authentication time to 1200 seconds.

```
Switch(config)#dot1x timeout re-authperiod 1200
```

5.2.2.17 dot1x timeout tx-period

Command: dot1x timeout tx-period <*seconds*>

no dot1x timeout tx-period

Function: Sets the interval for the supplicant to re-transmit EAP request/identity frame; the "**no dot1x timeout tx-period**" command restores the default setting.

Parameters: <*seconds*> is the interval for re-transmission of EAP request frames, in seconds; the valid range is 1 to 65535.

Command mode: Global Mode

Default: The default value is 30 seconds.

Usage Guide: Default value is recommended.

Example: Setting the EAP request frame re-transmission interval to 1200 seconds.

```
Switch(config)#dot1x timeout tx-period 1200
```

5.2.2.18 dot1x unicast enable

Command: dot1x unicast enable

no dot1x unicast enable

Function: Enable the switch forwarding 802.1x packets that with a unicast destination address in global. The "**no dot1x unicast enable** " command disables this function.

Parameters: Global Mode.

Default: Disable the switch forwarding 802.1x packets that with a unicast destination address in global mode.

Usage Guide: If want to enable forwarding 802.1x packets that with a unicast destination address for a port, you should enable the 802.1x function in global first, then enable the switch forwarding 802.1x packets that with a unicast destination address in global, and config the 802.1x for correspond port finally.

Example: Enable the switch forwarding 802.1x packets that with a unicast destination address, and enable 802.1x for port 1/1.

```
Switch(config)#dot1x enable
Switch(config)#dot1x unicast enable
Switch(config)#interface Ethernet 1/1
Switch(Config-If-Ethernet1/1)#dot1x enable
```

5.2.2.19 dot1x web authentication enable

Command：dot1x web authentication enable

no dot1x web authentication enable

Function：Enable Web authentication agent, the “**no dot1x web authentication enable”** command disable Web authentication agent.

Parameters：None.

Default：Web authentication agent is disabled.

Command mode：Global Mode

Usage Guide：Dot1x function must be enabled before enabling Web authentication agent. When dot1x web authentication agent is enabled, the “**dot1x privateclient enable** “ command should not be configured.

Example：Enable the Web authentication agent function.

```
Switch(config)#dot1x web authentication enable
```

5.2.2.20 dot1x web redirect

Command：dot1x web redirect <*URL*>

no dot1x web redirect

Function：Set the HTTP server address for Web redirection, the **“no dot1x web redirect”** command clear the address.

Parameters：*<URL>* is HTTP server address, in dotted decimal notation.

Default：The redirection function is disabled.

Command mode：Global Mode

Usage Guide：The Web authentication function must be enabled before setting the Web server address.The URL format is “http://A.B.C.D[:E]/F”,A.B.C.D is the IP address; E is the HTTP service port number, default value is 80;F is a string of character and the command do not do the validation checking on it.

Example： Set the Web redirction address as http://192.168.20.20/WebSupplicant/.

Switch(config)#dot1x web redirect http://192.168.20.20/WebSupplicant/

5.2.2.21 dot1x web redirect enable

Command: dot1x web redirect enable

no dot1x web redirect enable

Function: To enable unauthenticated user to visit Web redirect function. After enable this function, if unauthenticated user try to visit Website resource not for free (The http visiting required destination port is 80 here), the switch can configure Web visiting redirect to specified website, then remind user to authenticate.

Parameter: None.

Command Mode: Global Mode.

Default: The unauthenticated user Web redirect function is disabled by default. Manager can configure redirect function in inter security management background system, this address can transmit to switch through private communication protocol between switch and background system.

Example: Enable the unauthenticated user to visit the redirect function through Web.

Switch(config)#dot1x web redirect enable

5.3 802.1x Application Example

5.3.1 Example of Guest Vlan Applications

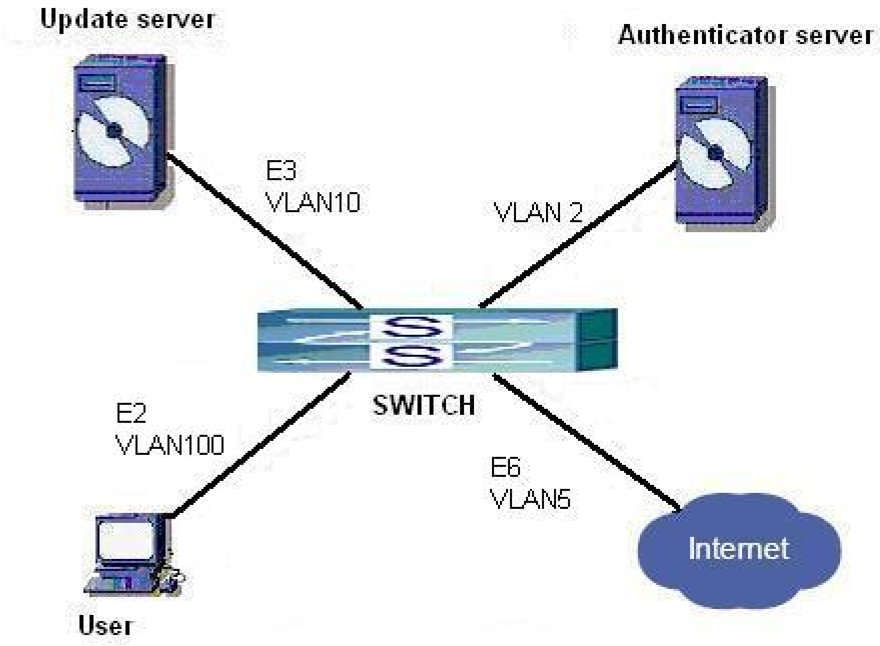


Fig 5-13 The Network Topology of Guest VLAN

Notes: in the figures in this session, E2 means Ethernet 1/2, E3 means Ethernet 1/3 and E6 means Ethernet 1/6.

As showed in the next figure, a switch accesses the network using 802.1x authentication, with a RADIUS server as its authentication server. Ethernet1/2, the port through which the user accesses the switch belongs to VLAN100; the authentication server is in VLAN2; Update Server, being in VLAN10, is for the user to download and update supplicant system software; Ethernet1/6, the port used by the switch to access the Internet is in VLAN5.

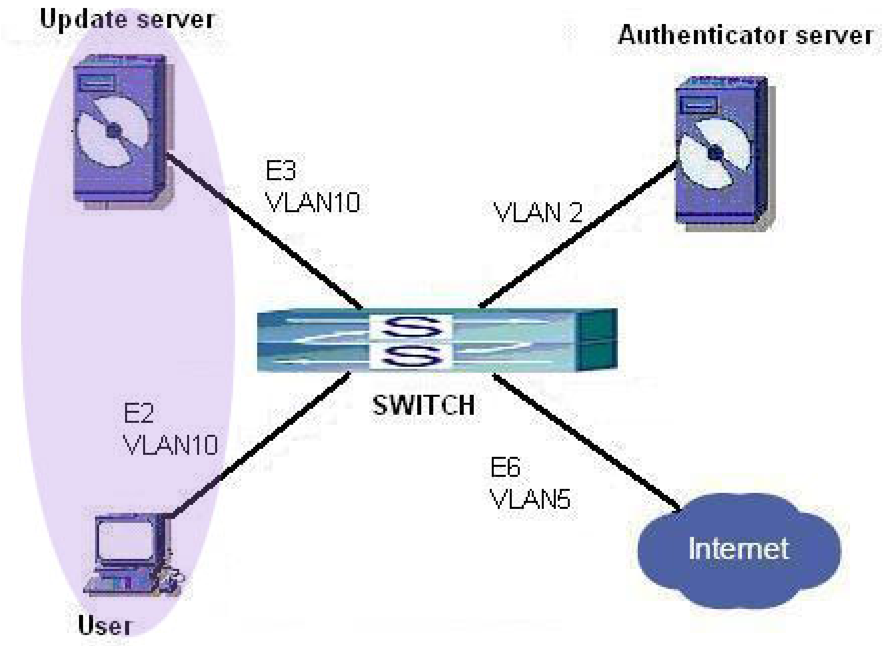


Fig 5-14 User Joining Guest VLAN

As illustrated in the up figure, on the switch port Ethernet1/2, the 802.1x feature is enabled, and the VLAN10 is set as the port’s Guest VLAN. Before the user gets authenticated or when the user fails to do so, port Ethernet1/2 is added into VLAN10, allowing the user to access the Update Server.

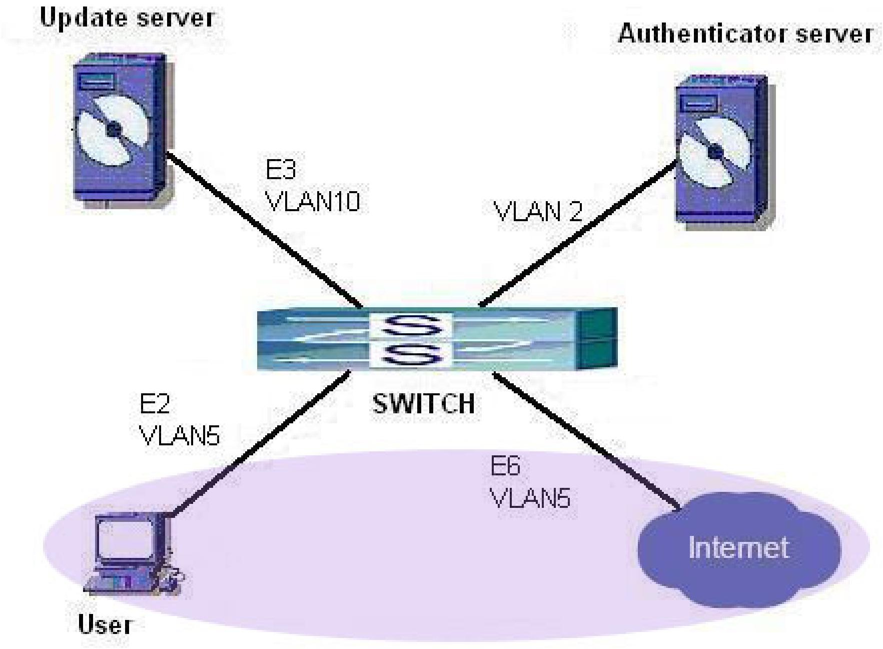


Fig 5-15 User Being Online, VLAN Being Offline

As illustrated in the up figure, when the users become online after a successful authentication, the authentication server will assign VLAN5, which makes the user and Etherne1/6 both in VLAN5, allowing the user to access the Internet.

The following are configuration steps:

```
# Configure RADIUS server.
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable

# Create VLAN100.
Switch(config)#vlan 100

# Enable the global 802.1x function
Switch(config)#dot1x enable

# Enable the 802.1x function on port Ethernet1/2
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#dot1x enable

# Set the link type of the port as access mode.
Switch(Config-If-Ethernet1/2)#switch-port mode access


# Set the access control mode on the port as portbased.
Switch(Config-If-Ethernet1/2)#dot1x port-method portbased


# Set the access control mode on the port as auto.
Switch(Config-If-Ethernet1/2)#dot1x port-control auto

# Set the port’s Guest VLAN as 100.
Switch(Config-If-Ethernet1/2)#dot1x guest-vlan 100
Switch(Config-If-Ethernet1/2)#exit
```

Using the command of **show running-config** or **show interface ethernet 1/2**, users can check the configuration of Guest VLAN. When there is no online user, no failed user authentication or no user gets offline successfully, and more authentication-triggering messages

(EAP-Request/Identity) are sent than the upper limit defined, users can check whether the Guest VLAN configured on the port takes effect with the command **show vlan id 100**.

5.3.2 Example of 802.1x and IPv4 Radius Applications

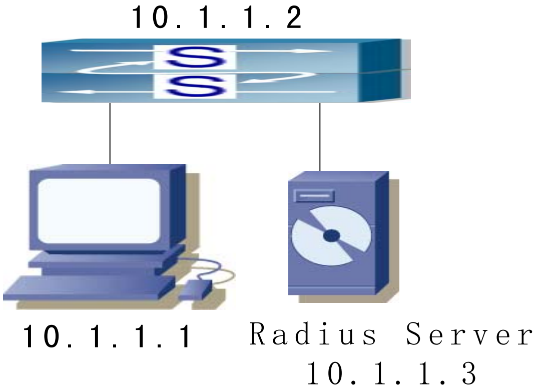


Fig 5-16 IEEE 802.1x Configuration Example Topology

The PC is connecting to port 1/2 of the switch; IEEE 802.1x authentication is enabled on port 1/2; the access mode is the default MAC-based authentication. The switch IP address is 10.1.1.2. Any port other than port 1/2 is used to connect to RADIUS authentication server, which has an IP address of 10.1.1.3, and use the default port 1812 for authentication and port 1813 for accounting. IEEE 802.1x authentication client software is installed on the PC and is used in IEEE 802.1x authentication.

The configuration procedures are listed below:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ip address 10.1.1.2 255.255.255.0
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 10.1.1.3
Switch(config)#radius-server accounting host 10.1.1.3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)#dot1x enable
Switch(Config-If-Ethernet1/2)#dot1x port-control auto
Switch(Config-If-Ethernet1/2)#exit
```

5.3.3 Example of 802.1x Web Proxy Authentication

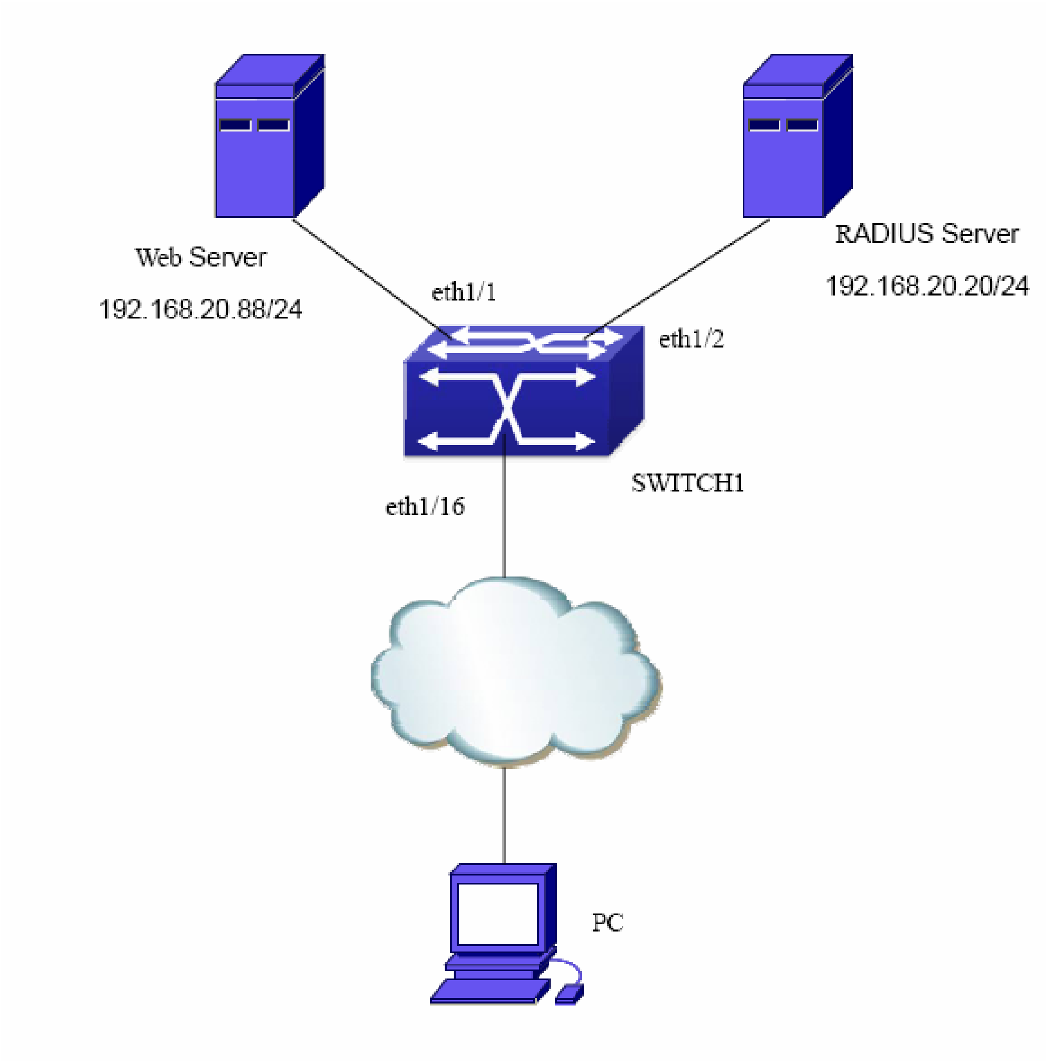


Fig 5-17 802.1x Web Proxy Authentication

In the network topology shown as above, Ethernet 1/1 on SWITCH1 is connected to the Web server whose IP address is 192.168.20.20/24, Ethernet 1/2 on SWITCH1 is connected to the RADIUS server whose IP address is 192.168.20.88/24 and authentication port is 1812. PC is connected to Ethernet 1/16 on SWITCH1 through an unknown network. The Web server and the authentication server are connected to VLAN 1, while PC is connected to VLAN 2. 802.1x Web authentication can be enabled through the following configuration. The re-authentication function is disabled by default. To enable this, corresponding 802.1x configuration should be issued first.

Configuration task list on SWITCH1

```
Switch(config)#dot1x enable
Switch(config)#dot1x web authentication enable
Switch(config)#dot1x web redirect http://192.168.20.20/WebSupplicant/
Switch(config)#interface ethernet 1/16
```

5.3.4 Example of DHCP Option82 Based 802.1x Authorization

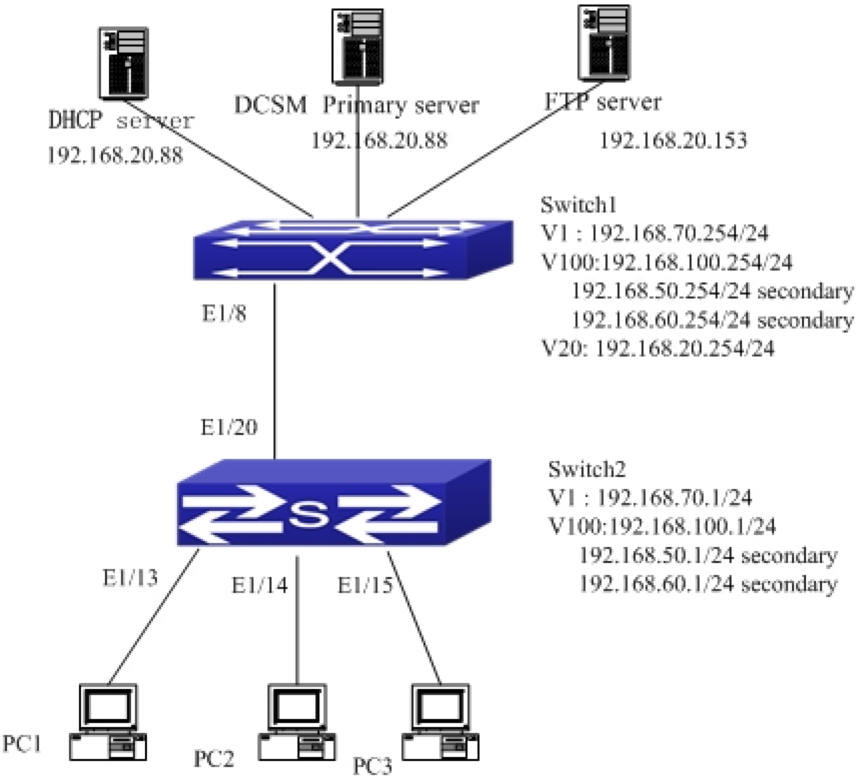


Fig 5-18 Topology for IEEE802.1x configuration

To enable DHCP option82 for address allocation on the DHCP server. To configure to make clients to get addresses in 192.168.50.0/24 before authentication, while get addresses in 192.168.100.0/24 after authentication.

Enable ACL for clients, only clients with the correct IP address and MAC address and the specified port number is allowed to be forwarded by the switch.

Suppose the network with address as 192.168.70.0/24 is the intranet. Non-authenticated clients which get IP address in 192.168.50.0.24 cannot communite with the hosts in intranet. This function can be implentmented through ACL on the trunk switches.

Requirements for the DHCP server: Redhat AS3 or Fedore Core 6, with ISC DHCP server installed. The version of the software should be 3.0.6 or above.

（1）Configuration for SWITCH2:

```
SWITCH2>en
SWITCH2#
SWITCH2#conf t
SWITCH2(config)#vlan 100
SWITCH2(Config-Vlan100)#switchport interface ethernet 1/13-24
SWITCH2(Config-Vlan100)#exit
SWITCH2(config)#interface vlan 1
SWITCH2(Config-if-Vlan1)#ip address 192.168.70.1 255.255.255.0
```

```
SWITCH2(Config-if-Vlan1)#exit
SWITCH2(config)#interface vlan 100
SWITCH2(Config-if-Vlan100)#ip address 192.168.100.1 255.255.255.0
SWITCH2(Config-if-Vlan100)#ip address 192.168.60.1 255.255.255.0 secondary
SWITCH2(Config-if-Vlan100)#ip address 192.168.50.1 255.255.255.0 secondary
SWITCH2(Config-if-Vlan100)#exit
SWITCH2(config)#ip route 192.168.20.0/24 192.168.100.254
SWITCH2(config)#ip dhcp snooping enable
SWITCH2(config)#ip dhcp snooping option82 enable
SWITCH2(config)#ip dhcp snooping binding enable
SWITCH2(config)#interface ethernet 1/20
SWITCH2(Config-If-Ethernet1/20)#ip dhcp snooping trust
SWITCH2(Config-If-Ethernet1/20)#exit
SWITCH2(config)#interface ethernet 1/13
SWITCH2(Config-If-Ethernet1/13)#ip dhcp snooping binding dot1x
SWITCH2(Config-If-Ethernet1/13)#exit
SWITCH2(config)#radius-server key test
SWITCH2(config)#radius-server authentication host 192.168.20.88
SWITCH2(config)#aaa enable
SWITCH2(config)#dot1x enable
SWITCH2(config)#dot1x privateclient enable
SWITCH2(config)#interface ethernet 1/13
SWITCH2(Config-If-Ethernet1/13)#dot1x enable
SWITCH2(Config-If-Ethernet1/13)#dot1x port-control auto
SWITCH2(Config-If-Ethernet1/13)#dot1x port-method dhcpoption82based
SWITCH2(Config-If-Ethernet1/13)#exit
SWITCH2(config)#exit
```

（2）Configuration for SWITCH1:

```
SWITCH1>
SWITCH1>en
SWITCH1#conf t
SWITCH1(config)#vlan 20
SWITCH1(Config-Vlan20)#switchport interface ethernet 0/0/9-23
SWITCH1(Config-Vlan20)#exit
SWITCH1(config)#vlan 100
SWITCH1(Config-Vlan100)#switchport interface ethernet 0/0/4-8
SWITCH1(Config-Vlan100)#exit
```

```
SWITCH1(config)#in
SWITCH1(config)#interface vlan 1
SWITCH1(Config-if-Vlan1)# ip address 192.168.70.254 255.255.255.0
SWITCH1(Config-if-Vlan1)#exit
SWITCH1(config)#interface vlan 20
SWITCH1(Config-if-Vlan20)#
SWITCH1(Config-if-Vlan20)# ip address 192.168.20.254 255.255.255.0
SWITCH1(Config-if-Vlan20)#exit
SWITCH1(config)#interface vlan 100
SWITCH1(Config-if-Vlan100)# ip address 192.168.100.254 255.255.255.0
SWITCH1(Config-if-Vlan100)#ip address 192.168.60.254 255.255.255.0 secondary
SWITCH1(Config-if-Vlan100)#ip address 192.168.50.254 255.255.255.0 secondary
SWITCH1(config)#exit
SWITCH1(config)#service dhcp
SWITCH1(config)#ip forward-protocol udp bootps
SWITCH1(config)#interface vlan 100
SWITCH1(Config-if-Vlan100)#ip helper-address 192.168.20.88
SWITCH1(Config-if-Vlan100)#exit
SWITCH1(config)#firewall enable
SWITCH1(config)#ip access-list extended denyua
SWITCH1(Config-IP-Ext-Nacl-denyua)#deny ip 192.168.50.0 0.0.0.255 192.168.70.0 0.0.0.255
SWITCH1(Config-IP-Ext-Nacl-denyua)#
SWITCH1(Config-IP-Ext-Nacl-denyua)#exit
SWITCH1(config)#interface ethernet 1/8
SWITCH1(Config-If-Ethernet1/8)#ip access-group denyua in
SWITCH1(Config-If-Ethernet1/8)#
```

（3）Example dhcp.conf file for DHCP server configuration:

```
ddns-update-style interim;
ignore client-updates;
authoritative;

#Authenticated clients
# To configure user authenticated option82 as authen in TrustView background accordingly.
class "AuthClass" {
    match if option agent.circuit-id = "authen";
}
#UnAuthenticated clients
```

```
# The switch auto added option82 function by default.
class "UnAuthClass" {
        match if option agent.circuit-id = "unauth";
}
shared-network subnet300{
        subnet 192.168.100.0 netmask 255.255.255.0 {
                option routers 192.168.100.254;
        }
        subnet 192.168.20.0 netmask 255.255.255.0 {
                option routers 192.168.20.254;
        }
        subnet 192.168.50.0 netmask 255.255.255.0 {
                option routers 192.168.50.254;
        }
        pool {
                range 192.168.100.100 192.168.100.200;
                max-lease-time 3000;
                allow members of "AuthClass";
        }
        pool {
                range 192.168.50.100 192.168.50.200;
                max-lease-time 3000;
                allow members of "UnAuthClass";
        }
        subnet 192.168.60.0 netmask 255.255.255.0 {
                option routers 192.168.60.254;
                pool {
                        range 192.168.60.100 192.168.60.200;
                        max-lease-time 3000;
                        deny members of "AuthClass";
                        deny members of "UnAuthClass";
                }
        }
```

5.3.5 802.1x Troubleshooting

It is possible that 802.1x be congfigured on ports and 802.1x authentication be setted to auto, but switch cann’t be to authenticated state after the user runs 802.1x supplicant software. Here are some possible causes and solutions:

- ☞ If 802.1x cannot be enabled for a port, make sure the port is not executing Spanning tree, or MAC binding, or configured as a port aggregation. To enable the 802.1x authentication, the above functions must be disabled.
- ☞ If the switch is configured properly but still cannot pass through authentication, connectivity between the switch and RADIUS server, the switch and 802.1x client should be verified, and the port and VLAN configuration for the switch should be checked, too.
- ☞ Check the event log in the RADIUS server for possible causes. In the event log, not only unsuccessful logins are recorded, but prompts for the causes of unsuccessful login. If the event log indicates wrong authenticator password, radius-server key parameter shall be modified; if the event log indicates no such authenticator, the authenticator needs to be added to the RADIUS server; if the event log indicates no such login user, the user login ID and password may be wrong and should be verified and input again.
- ☞ Too frequent access to RADIUS data such as run “show aaa” commands may cause the user to be unable to pass through the authentication due to RADIUS data share violation. And the same reason may force users to go offline on re-authentication in the use. As a result, it is recommended to minimize operation to RADIUS data when users are authenticating or re-authenticating.
- ☞ It is required that private 802.1x authentication client software and the intranet security management system – TrustView, as well as the DHCP server, should be ready before DHCP option82 based 802.1x authentication can be configured. By default, if DHCP option 82 is enabled, the switch will fill the remote-id field of DHCP option82 as unauth, and circuit-id as the MAC address of the CPU port of the switch when the client has not been authenticated. After the client passes the authentication, the remote-id field of option 82 messages of DHCP request messages, will be determined by the intranet security management system. Also, the circuit-id field will be the MAC address of the CPU port. Before the configuration can work, DHCP server must be configured correctly and both the address pools for the un-authenticated clients and authenticated clients should be ready. After DHCP option 82 based 802.1x authentication, debugging messages can be enabled through the command debug dot1x detail dhcp option82 based.

5.3.5.1 Commands for 802.1X

5.3.5.1.1 debug dot1x detail

Command：debug dot1x detail { pkt-send | pkt-receive | internal | all | userbased | webbased |dhcpoption82based } interface [ethernet] <*interface-name*>

no debug dot1x detail { pkt-send | pkt-receive | internal | all | userbased | webbased |dhcpoption82based } interface [ethernet] <*interface-name*>

Function: Enable the debug information of dot1x details; the no operation of this command will disable that debug information.

Parameters：pkt-send: Enable the debug information of dot1x about sending packets;

pkt-receive: Enable the debug information of dot1x about receiving packets;

internal: Enable the debug information of dot1x about internal details;

all: Enable the debug information of dot1x about all details mentioned above;

userbased： user-based authentication;

webbased： Web-based authentication;

dhcpoption82based: the access control method based on dhcp option82;

<*interface-name*>: the name of the interface.

Command Mode： Admin Mode.

Usage Guide： By enabling the debug information of dot1x details, users can check the detailed processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example： Enable all debug information of dot1x details on interface1/1.

```
Switch#debug dot1x detail all interface ethernet1/1
```

5.3.5.1.2 debug dot1x error

Command：debug dot1x error

no debug dot1x error

Function：Enable the debug information of dot1x about errors; the no operation of this command will disable that debug information.

Parameters： None.

Command Mode： Admin Mode.

Usage Guide： By enabling the debug information of dot1x about errors, users can check the information of errors that occur in the processes of the Radius protocol operation, which might help diagnose the cause of faults if there is any.

Example： Enable the debug information of dot1x about errors.

```
Switch#debug dot1x error
```

5.3.5.1.3 debug dot1x fsm

Command：debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <*interface-name*>

no debug dot1x fsm {all | aksm | asm | basm | ratsm} interface <*interface-name*>

Function： Enable the debug information of dot1x state machine; the no operation of this command will disable that debug information.

Command Mode： Admin Mode.

Parameters：all： Enable the debug information of dot1x state machine;

aksm： Enable the debug information of Authenticator Key Transmit state machine;

asm： Enable the debug information of Authenticator state machine;

basm： Enable the debug information of Backend Authentication state machine;

ratsm： Enable the debug information of Re-Authentication Timer state machine;

<*interface-name*>： the name of the interface.

Usage Guide： By enabling the debug information of dot1x, users can check the negotiation process of dot1x protocol, which might help diagnose the cause of faults if there is any.

Example： Enable the debug information of dot1x state machine.

```
Switch#debug dot1x fsm asm interface ethernet1/1
```

5.3.5.1.4 debug dot1x packet

Command：debug dot1x packet {all | receive | send} interface <*interface-name*>

no debug dot1x packet {all | receive | send} interface <*interface-name*>

Function： Enable the debug information of dot1x about messages; the no operation of this command will disable that debug information.

Command Mode： Admin Mode.

Parameters：send： Enable the debug information of dot1x about sending packets;

receive： Enable the debug information of dot1x about receiving packets;

all： Enable the debug information of dot1x about both sending and receiving packets;

<*interface-name*>: the name of the interface.

Usage Guide： By enabling the debug information of dot1x about messages, users can check the negotiation process of dot1x protocol, which might help diagnose the cause of faults if there is any.

Example： Enable the debug information of dot1x about messages.

```
Switch#debug dot1x packet all interface ethernet1/1
```

5.3.5.1.5 show dot1x

Command: show dot1x [interface <*interface-list*>]

Function: Displays dot1x parameter related information, if parameter information is added, corresponding dot1x status for corresponding port is displayed.

Parameters: <*interface-list*> is the port list. If no parameter is specified, information for all ports is displayed.

Command mode: Admin Mode

Usage Guide: The dot1x related parameter and dot1x information can be displayed with “show dot1x” command.

Example:

1. Display information about dot1x global parameter for the switch.

```
Switch#show dot1x
Global 802.1x Parameters
reauth-enabled          no
reauth-period           3600
quiet-period            10
tx-period               30
max-req                 2
authenticator mode      passive
Mac Filter Disable
MacAccessList :
dot1x-EAPoR Enable
802.1x is enabled on ethernet 1
Authentication Method:Port based
Status                  Authorized
Port-control            Auto
Supplicant              00-03-0F-FE-2E-D3
Authenticator State Machine
   State                    Authenticated
Backend State Machine
   State                    Idle
Reauthentication State Machine
   State                    Stop
```

Displayed information	Explanation
Global 802.1x Parameters	Global 802.1x parameter information
reauth-enabled	Whether re-authentication is enabled or not
reauth-period	Re-authentication interval
quiet-period	Silent interval
tx-period	EAP retransmission interval
max-req	EAP packet retransmission interval
authenticator mode	Switch authentication mode
Mac Filter	Enables dot1x address filter or not
MacAccessList	Dot1x address filter table
Dot1x-EAPoR	Authentication method used by the switch (EAP relay, EAP local end)
802.1x is enabled on ethernet 1	Indicates whether dot1x is enabled for the port
Authentication Method:	Port authentication method (MAC-based, port-based)

Status	Port authentication status
Port-control	Port authorization status
Supplicant	Authenticator MAC address
Authenticator State Machine	Authenticator state machine status
Backend State Machine	Backend state machine status
Reauthentication State Machine	Re-authentication state machine status

5.4 Web Management

Click “Authentication configuration”, to open authentication configuration management list. Users may configure switch 802.1x authentication function.

5.4.1 802.1X configuration

Click “Authentication configuration”, “802.1X configuration” to open the 802.1x function configuration management list and configure the switch 802.1x function.

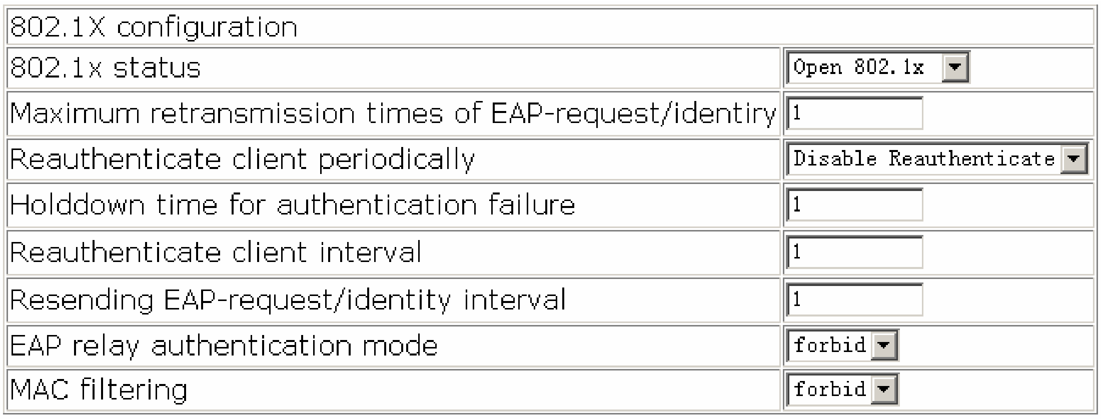
5.4.1.1 802.1X configuration

Click “Authentication configuration”, “802.1X configuration”, “802.1X configuration” to configure the 802.1x global configurations:

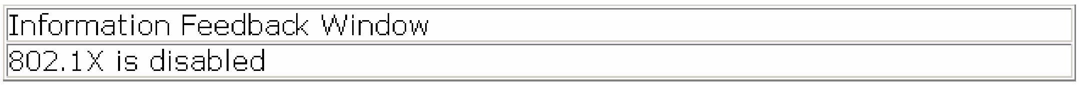
- 802.1x status -Enables, disables the switch 802.1x function.
- Maximum retransmission times of EAP-request/identity(1-10 second) - Configures sending EAP-request/MD5 frame the maximum times before switch did not receive suppliant response and restart authentication.
- Re-authenticate client periodically - permit, forbid to make seasonal re-authentication for suppliant.
- Holddown time for authentication failure(1-65535 second) - Configures suppliant quiet-period status time after authentication failure.
- Re-authenticate client interval(1-65535 second) - Configures time interval of switch re-authentication client.
- Resending EAP-request/identity interval(1-65535 second) - Configures time interval of switch retransfer EAP-request/identity frame to suppliant.
- EAP relay authentication mode - Configures switch to adopt EAP relay method to make authentication; use the “no” command to configure switch to adopt EAP local terminating method to make authentication.
- MAC filtering -Enables, disables the switch dot1x address filter function.

Example: Choose 802.1x status as Open 802.1x, Configure Maximum retransmission times of

EAP-request/identity as 1, choose Re-authenticate client periodically as Disable Re-authenticate, configure Holddown time for authentication failure as 1, configure Reauthenticate client interval as 1, configure Resending EAP-request/identity interval as 1, choose EAP relay authentication mode as forbid, choose MAC filtering as forbid and then click Apply button to set the configurations.



802.1X configuration	
802.1x status	Open 802.1x ▼
Maximum retransmission times of EAP-request/identiry	1
Reauthenticate client periodically	Disable Reauthenticate ▼
Holddown time for authentication failure	1
Reauthenticate client interval	1
Resending EAP-request/identity interval	1
EAP relay authentication mode	forbid ▼
MAC filtering	forbid ▼



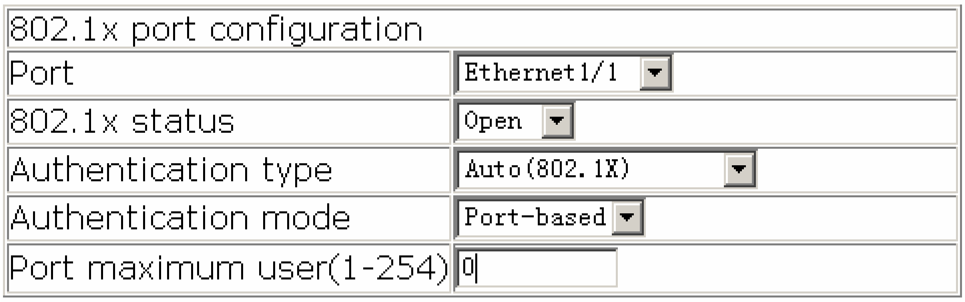
Information Feedback Window
802.1X is disabled

5.4.1.2 802.1x port authentication configuration

Click “Authentication configuration”, “802.1X configuration”, “802.1X portauthentication configuration” to C onfigure port 802.1x function

- Port -assigns port
- 802.1x status -port 802.1x status, Open, 802.1x function is open; Close, 802.1x function is close.
- Authentication type - Configures port 802.1x authentication status. Auto means enable 802.1x authentication. According to switch and suppliant authentication information, to confirm that the port is in authenticated status or unauthenticated status, force-authorized is configured port as authenticated status, allowing unauthenticated data to pass across the port; for force-unauthorized configure port unauthenticated status, switch not provide suppliant authentication service in this port, not permit any port pass across this port.
- Authentication mode -Configures the access control method for a specific port. Mac-based is access control method which is based on MAC address; port-based access control method which is based on port.
- Port maximum user(1-254) - Configures the permission maximum user for specific port.

Example: Choose Ethernet port1/1, choose 802.1x status as Open, choose Authentication type as auto, choose Authentication mode as port based, configure Port maximum user as 10 and then click the Set button to apply this configuration to switch.



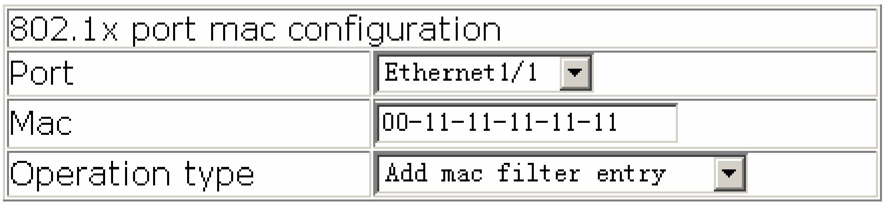
802.1x port configuration	
Port	Ethernet1/1
802.1x status	Open
Authentication type	Auto(802.1X)
Authentication mode	Port-based
Port maximum user(1-254)	0

5.4.1.3 802.1x port mac configuration

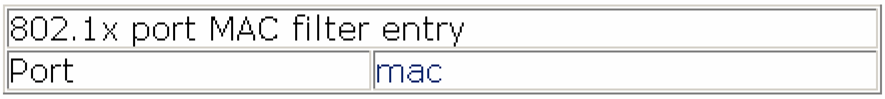
Click “Authentication configuration”, “802.1X configuration”, “802.1x port mac configuration” to Add a MAC address table to dot1x address filter.

- Port -If specify port, the added list only suitable for specific port, specify All Ports, the added list suitable for all port.
- Mac -adds MAC address
- Operation type -adds, removes filter MAC

Example: Choose Ethernet port 1/1, configure MAC as 00-11-11-11-11-11, choose Operation type as Add mac filter entry, and then click the Apply button to apply this configuration to switch.



802.1x port mac configuration	
Port	Ethernet1/1
Mac	00-11-11-11-11-11
Operation type	Add mac filter entry



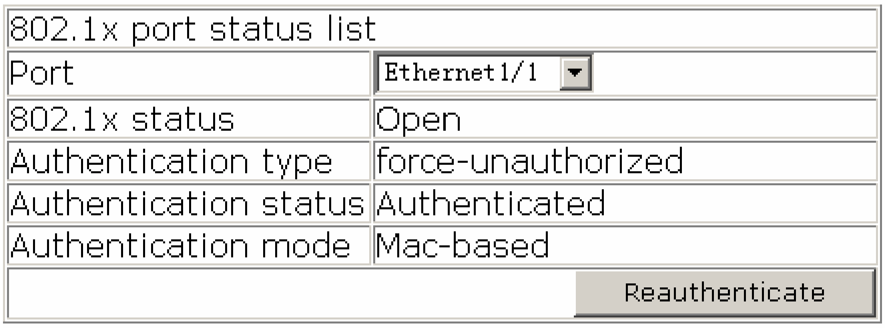
802.1x port MAC filter entry	
Port	mac

5.4.1.4 802.1x port status list

Click “Authentication configuration”, “802.1X configuration”, and “802.1x port status list” to display port 802.1x configuration information, and make re-authentication for the specific port.

- Port -assign port
- 802.1x status -port 802.1x status
- Authentication type -Authentication type
- Authentication status -Authentication status
- Authentication mode -Authentication mode

Example: Choose Ethernet port 1/1, then Click Reauthenticate button, the user in Ethernet port 1/1 will be force to make re-authentication.



802.1x port status list	
Port	Ethernet1/1 ▼
802.1x status	Open
Authentication type	force-unauthorized
Authentication status	Authenticated
Authentication mode	Mac-based

Chapter 6 The Number Limitation Function Of Port, MAC in VLAN and IP Configuration

6.1 Introduction to the Number Limitation Function of Port, MAC in VLAN and IP

MAC address list is used to identify the mapping relationship between the destination MAC addresses and the ports of switch. There are two kinds of MAC addresses in the list: static MAC address and dynamic MAC address. The static MAC address is set by users, having the highest priority (will not be overwritten by dynamic MAC address), and will always be effective; dynamic MAC address is learnt by the switch through transmitting data frames, and will only be effective in a specific time range. When the switch receives a data framed waiting to be transmitted, it will study the source MAC address of the data frame, build a mapping relationship with the receiving port, and then look up the MAC address list for the destination MAC address. If any matching list entry is found, the switch will transmit the data frame via the corresponding port, or, the switch will broadcast the data frame over the VLAN it belongs to. If the dynamically learnt MAC address matches no transmitted data in a long time, the switch will delete it from the MAC address list.

Usually the switch supports both the static configuration and dynamic study of MAC address, which means each port can have more than one static set MAC addresses and dynamically learnt MAC addresses, and thus can implement the transmission of data traffic between port and known MAC addresses. When a MAC address becomes out of date, it will be dealt with broadcast. No number limitation is put on MAC address of the ports of our current switches; every port can have several MAC addressed either by configuration or study, until the hardware list entries are exhausted. To avoid too many MAC addresses of a port, we should limit the number of MAC addresses a port can have.

For each INTERFACE VLAN, there is no number limitation of IP; the upper limit of the number of IP is the upper limit of the number of user on an interface, which is, at the same time, the upper limit of ARP and ND list entry. There is no relative configuration command can be used to control the sent number of these list entries. To enhance the security and the controllability of our products, we need to control the number of MAC address on each port and the number of ARP, ND on each INTERFACE VLAN. The number of static or dynamic MAC address on a port should not exceed the configuration. The number of user on each VLAN should not exceed the configuration, either.

Limiting the number of MAC and ARP list entry can avoid DOS attack to a certain extent.

When malicious users frequently do MAC or ARP cheating, it will be easy for them to fill the MAC and ARP list entries of the switch, causing successful DOS attacks.

To summer up, it is very meaningful to develop the number limitation function of port, MAC in VLAN and IP. ES4700BD series switch can control the number of MAC address of ports and the number ARP, ND list entry of ports and VLAN through configuration commands.

Limiting the number of dynamic MAC and IP of ports:

1. Limiting the number of dynamic MAC. If the number of dynamically learnt MAC address by the switch is already larger than or equal with the max number of dynamic MAC address, then shutdown the MAC study function on this port, otherwise, the port can continue its study.

2. Limiting the number of dynamic IP. If the number of dynamically learnt ARP and ND by the switch is already larger than or equal with the max number of dynamic ARP and ND, then shutdown the ARP and ND study function of this port, otherwise, the port can continue its study.

Limiting the number of dynamic MAC and IP of interfaces:

1. Limiting the number of dynamic MAC. If the number of dynamically learnt MAC address by the VLAN of the switch is already larger than or equal with the max number of dynamic MAC address, then shutdown the MAC study function of all the ports in this VLAN, otherwise, all the ports in this VLAN can continue their study (except special ports).

2. Limiting the number of dynamic IP. If the number of dynamically learnt ARP and ND by the switch is already larger than or equal with the max number of dynamic ARP and ND, then the VLAN will not study any new ARP or ND, otherwise, the study can be continued.

6.2 The Number Limitation Function of Port, MAC in VLAN and IP Configuration Task List

1. Enable the number limitation function of MAC、IP on ports
2. Enable the number limitation function of MAC、IP in VLAN
3. Configure the timeout value of querying dynamic MAC.
4. Display and debug the relative information of number limitation of MAC、IP on ports

1. Enable the number limitation function of MAC、IP on ports

Command	Explanation
Port configuration mode	
switchport mac-address dynamic maximum <value> **no switchport mac-address dynamic maximum**	Enable and disable the number limitation function of MAC on the ports

switchport arp dynamic maximum <value> **no switchport arp dynamic maximum**	Enable and disable the number limitation function of ARP on the ports
switchport nd dynamic maximum <value> **no switchport nd dynamicmaximum**	Enable and disable the number limitation function of ND on the ports

2. Enable the number limitation function of MAC、IP in VLAN

Command	Explanation
Interface configuration mode	
vlan mac-address dynamic maximum <value> **no vlan mac-address dynamic maxim um**	Enable and disable the number limitation function of MAC in the VLAN
ip arp dynamic maximum <value> **no ip arp dynamic maximum**	Enable and disable the number limitation function of ARP in the VLAN
Ipv6 nd dynamic maximum <value> **no ipv6 nd dynamic maximum**	Enable and disable the number limitation function of NEIGHBOR in the VLAN

3. Configure the timeout value of querying dynamic MAC.

Command	Explanation
Global configuration mode	
mac-address query timeout <seconds>	Configure the timeout value of querying dynamic MAC.

4. Display and debug the relative information of number limitation of MAC、IP on ports

Command	Explanation
Admin mode	
show mac-address dynamic count {vlan <vlan-id>|interface ethernet <portName>}	Display the number of dynamic MAC in corresponding ports and VLAN

show arp-dynamic count {vlan <vlan-id>|interface ethernet <portName>}	Display the number of dynamic ARP in corresponding ports and VLAN
show nd-dynamic count {vlan <vlan-id>|interface ethernet <portName>}	Display the number of dynamic NEIGHBOUR in corresponding ports and VLAN
debug switchport mac count **no debug switchport mac count**	All kinds of debug information when limiting the number of MAC on ports
debug switchport arp count **no debug switchport arp count**	All kinds of debug information when limiting the number of ARP on ports
debug switchport nd count **no debug switchport nd count**	All kinds of debug information when limiting the number of NEIGHBOUR on ports
debug vlan mac count **no debug vlan mac count**	All kinds of debug information when limiting the number of MAC in VLAN
debug ip arp count **no debug switchport mac count**	All kinds of debug information when limiting the number of ARP in VLAN
debug ipv6 nd count **no debug switchport mac count**	All kinds of debug information when limiting the number of NEIGHBOUR in VLAN

6.3 Command for The Number Limitation Function of Port, MAC in VLAN and IP

6.3.1 switchport mac-address dynamic maximum

Command：switchport mac-address dynamic maximum <*value*>

no switchport mac-address dynamic maximum

Function：Set the max number of dynamic MAC address allowed by the port, and, at the same time, enable the number limitation function of dynamic MAC address on the port; “no switchport mac-address dynamic maximum” command is used to disable the number limitation function of dynamic MAC address on the port.

Parameters：<*value*> upper limit of the number of dynamic MAC address of the port, ranging from 1 to 4096.

Default Settings：The number limitation function of dynamic MAC address on the port is disabled.

Command Mode： Port mode.

Usage Guide： When configuring the max number of dynamic MAC address allowed by the port, if the number of dynamically learnt MAC address on the port is already larger than the max number of dynamic MAC address to be set, the extra dynamic MAC addresses will be deleted. This function is mutually exclusive to functions such as dot1x, MAC binding, if the functions of dot1x, MAC binding or TRUNK are enabled on the port, this function will not be allowed.

Examples：

Enable the number limitation function of dynamic MAC address in port 1/2 mode, the max number to be set is 20

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)# switchport mac-address dynamic maximum 20
```

Disable the number limitation function of dynamic MAC address in port 1/2 mode.

```
Switch(Config-If-Ethernet1/2)#no switchport mac-address dynamic maximum
```

6.3.2 vlan mac-address dynamic maximum

Command：vlan mac-address dynamic maximum <*value*>
no vlan mac-address dynamic maximum

Function： Set the max number of dynamic MAC address allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic MAC address in the VLAN; "no vlan mac-address dynamic maximum" command is used to disable the number limitation function of dynamic MAC address in the VLAN.

Parameters：<*value*> upper limit of the number of MAC address in the VLAN, ranging from 1 to 4096.

Default Settings： The number limitation function of dynamic MAC address in the VLAN is disabled.

Command Mode： VLAN mode.

Usage Guide： When configuring the max number of dynamic MAC allowed in the VLAN, if the number of dynamically learnt MAC address in the VLAN is already larger than the max number to be set, the extra dynamic MAC addresses will be deleted. After enabling number limitation function of dynamic MAC in the VLAN, the number limitation of MAC is only applied to general access port, the number of MAC on TURNK ports and special ports which has enabled dot1x, MAC binding function will not be limited or counted.

Examples：

Enable the number limitation function of dynamic MAC address in VLAN 1, the max number to be set is 50.

```
Switch(config)#vlan 1
Switch(Config-Vlan1)# vlan mac-address dynamic maximum 50
```

Enable the number limitation function of dynamic MAC address in VLAN 1.

```
Switch(Config-Vlan1)#no vlan mac-address dynamic maximum
```

6.3.3 switchport arp dynamic maximum

Command：switchport arp dynamic maximum <*value*>

no switchport arp dynamic maximum

Function：Set the max number of dynamic ARP allowed by the port, and, at the same time, enable the number limitation function of dynamic ARP on the port; “no switchport arp dynamic maximum” command is used to disable the number limitation function of dynamic ARP on the port.

Parameters：<*value***>** upper limit of the number of dynamic ARP of the port, ranging from 1 to 4096.

Default Settings：The number limitation function of dynamic ARP on the port is disabled.

Command Mode：Port mode.

Usage Guide：When configuring the max number of dynamic ARP allowed by the port, if the number of dynamically learnt ARP on the port is already larger than the max number to be set, the extra dynamic ARP will be deleted. TRUNK ports do not supports this function.

Examples：

Enable the number limitation function of dynamic ARP in port 1/2 mode, the max number to be set is 20

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)# switchport arp dynamic maximum 20
```

Disable the number limitation function of dynamic ARP in port 1/2 mode.

```
Switch(Config-If-Ethernet1/2)#no switchport arp dynamic maximum
```

6.3.4 switchport nd dynamic maximum

Command：switchport nd dynamic maximum <*value*>

no switchport nd dynamic maximum

Function：Set the max number of dynamic NEIGHBOR allowed by the port, and, at the same time, enable the number limitation function of dynamic NEIGHBOR on the port; “no switchport nd dynamic maximum” command is used to disable the number limitation function of dynamic NEIGHBOR on the port.

Parameters：<*value***>** upper limit of the number of dynamic NEIGHBOR of the port, ranging from 1 to 4096.

Default Settings：The number limitation function of dynamic ARP on the port is disabled.

Command Mode：Port mode.

Usage Guide：When configuring the max number of dynamic NEIGHBOR allowed by the port, if the number of dynamically learnt NEIGHBOR on the port is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted. TRUNK ports do not supports this function.

Examples：

Enable the number limitation function of dynamic NEIGHBOR in port 1/2 mode, the max number to be

20.

```
Switch(config)#interface ethernet 1/2
Switch(Config-If-Ethernet1/2)# switchport nd dynamic maximum 20
```

Disable the number limitation function of dynamic NEIGHBOR in port 1/2 mode.

```
Switch(Config-If-Ethernet1/2)#no switchport nd dynamic maximum
```

6.3.5 ip arp dynamic maximum

Command：ip arp dynamic maximum <*value*>

no ip arp dynamic maximum

Function：Set the max number of dynamic ARP allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic ARP in the VLAN; “no ip arp dynamic maximum” command is used to disable the number limitation function of dynamic ARP in the VLAN.

Parameters：<*value*> upper limit of the number of dynamic ARP in the VLAN, ranging from 1 to 4096.

Default Settings：the number limitation function of dynamic ARP in the VLAN is disabled.

Command Mode：Interface mode.

Usage Guide：When configuring the max number of dynamic ARP allowed in the VLAN, if the number of dynamically learnt ARP in the VLAN is already larger than the max number to be set, the extra dynamic ARP will be deleted.

Examples：

Enable the number limitation function of dynamic ARP in VLAN 1, the max number to be set is 50

```
Switch(config)#interface ethernet 1/2
Switch(Config-if-Vlan1)# ip arp dynamic maximum 50
```

Disable the number limitation function of dynamic ARP in VLAN 1

```
Switch(Config-if-Vlan1)#no ip arp dynamic maximum
```

6.3.6 ipv6 nd dynamic maximum

Command：ipv6 nd dynamic maximum <*value*>

no ipv6 nd dynamic maximum

Function：Set the max number of dynamic NEIGHBOR allowed in the VLAN, and, at the same time, enable the number limitation function of dynamic NEIGHBOR in the VLAN; “no ipv6 nd dynamic maximum” command is used to disable the number limitation function of dynamic NEIGHBOR in the VLAN.

Parameters：<*value*> upper limit of the number of dynamic NEIGHBOR in the VLAN, ranging from 1 to 4096.

Default Settings：the number limitation function of dynamic NEIGHBOR in the VLAN is disabled.

Command Mode：Interface mode.

Usage Guide：When configuring the max number of dynamic NEIGHBOR allowed in the VLAN, if the number of dynamically learnt NEIGHBOR in the VLAN is already larger than the max number to be set, the extra dynamic NEIGHBOR will be deleted.

Examples：

Enable the number limitation function of dynamic NEIGHBOR in VLAN 1, the max number to be set is 50

Switch(config)#interface ethernet 1/2

Switch(Config-if-Vlan1)# ipv6 nd dynamic maximum 50

Disable the number limitation function of dynamic NEIGHBOR in VLAN 1

Switch(Config-if-Vlan1)#no ipv6 nd dynamic maximum

6.3.7 mac-address query timeout

Command：mac-address query timeout <*seconds*>

Function：Set the timeout value of querying dynamic MAC

Parameter：<*seconds*> is timeout value, in second, ranging from 5 to 300

Default Settings：Default value is 60 seconds

Command Mode：Global mode

Usage Guide：After enabling the number limitation of MAC, users can use this command to configure the timeout value of querying dynamic MAC. If the data traffic is very large, the timeout value can be shorter, otherwise, it can be longer. Users can set it according to actual situation.

Examples：

Set the timeout value of quering dynamic MAC as 30 seconds

Switch(config)# mac-address query timeout 30

6.3.8 show mac-address dynamic count

Command：show mac-address dynamic count { (vlan <1-4096>)| interface ethernet <*portName*>}

Function：Display the number of dynamic MAC of corresponding port and VLAN.

Parameters：<*vlan-id*>display the specified vlan ID. **<*portName*>** is the name of layer-2 port

Command Mode：Admin Mode

Usage Guide：Use this command to display the number of dynamic MAC of corresponding port and VLAN.

Examples：Display the number of dynamic MAC of the port and VLAN which are configured with number limitation function of MAC

```
Switch(config)# show mac-address dynamic count interface ethernet 1/3
 Port                MaxCount                CurrentCount
----------------------------------------------------------------------------------------------------
 Ethernet1/3                5                     1
----------------------------------------------------------------------------------------------------
Switch(config)# show mac-address dynamic count vlan 1
 Vlan                MaxCount                CurrentCount
----------------------------------------------------------------------------------------------------
 1                       55                    15
----------------------------------------------------------------------------------------------------
```

6.3.9 show arp-dynamic count

Command：show arp-dynamic count { (vlan <1-4096>)| interface ethernet <*portName*>}

Function：Display the number of dynamic ARP of corresponding port and VLAN.**Parameters：** ***<vlan-id>*** is play the specified vlan ID.***<portName>*** is the name of layer-2 port

Command Mode：Admin Mode

Usage Guide：Use this command to display the number of dynamic ARP of corresponding port and VLAN.

Examples：Display the number of dynamic ARP of the port and VLAN which are configured with number limitation function of ARP

```
Switch(config)# show arp-dynamic count interface ethernet 1/3
 Port                MaxCount                CurrentCount
----------------------------------------------------------------------------------------------------
 Ethernet1/3                5                     1
----------------------------------------------------------------------------------------------------
Switch(config)# show arp-dynamic count vlan 1
 Vlan                MaxCount                CurrentCount
----------------------------------------------------------------------------------------------------
 1                       55                    15
----------------------------------------------------------------------------------------------------
```

6.3.10 show nd-dynamic count

Command：show nd-dynamic count { (vlan <1-4096>)| interface ethernet <*portName*>}

Function：Display the number of dynamic ND of corresponding port and VLAN.

Parameters：*<vlan-id>* is play the specified vlan ID.***<portName>*** is the name of layer-2 port

Command Mode：Admin Mode

Usage Guide：Use this command to display the number of dynamic ND of corresponding port and VLAN.

Examples：Display the number of dynamic ND of the port and VLAN which are configured with number limitation function of ND

```
Switch(config)# show nd-dynamic count interface ethernet 1/3
 Port               MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 Ethernet1/3                5                    1
-------------------------------------------------------------------------------------------------
Switch(config)# show nd-dynamic count vlan 1
 Vlan               MaxCount                CurrentCount
-------------------------------------------------------------------------------------------------
 1                        55                  15
-------------------------------------------------------------------------------------------------
```

6.3.11 debug switchport mac count

Command：debug switchport mac count

no debug switchport mac count

Function：When the number limitation function debug of mac on the port, if the number of dynamic MAC and the number of MAC on the port is larger than the max number allowed, users will see debug information.” no debug switchport mac count” command is used to disable the number limitation function debug of mac on the port.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic mac on the port

Examples：

```
Switch#debug switchport mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in port Ethernet3/1
!!%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!
```

6.3.12 debug switchport arp count

Command：debug switchport arp count

no debug switchport arp count

Function：When the number limitation function debug of arp on the port, if the number of dynamic arp and the number of arp on the port is larger than the max number allowed, users will see debug information.” no debug switchport arp count” command is used to disable the number limitation function debug of arp on the port.

Parameters：**None**

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic arp on the port

Examples：

```
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in port
Ethernet3/1
!!%Jun 14 16:04:40 2007 Arp learning will be stopped and some mac will be delete !!
```

6.3.13 debug switchport nd count

Command：**debug switchport nd count**

no debug switchport nd count

Function：When the number limitation function debug of nd on the port, if the number of dynamic nd and the number of nd on the port is larger than the max number allowed, users will see debug information.” no debug switchport nd count” command is used to disable the number limitation function debug of nd on the port.

Parameters：**None**

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic nd on the port

Examples：

```
Switch#debug switchport arp count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in
port Ethernet3/1
!!%Jun 14 16:04:40 2007 Neighbor learning will be stopped and some mac will be delete !!
```

6.3.14 debug vlan mac count

Command：**debug vlan mac count**

no debug vlan mac count

Function：When the number limitation function debug of mac in the VLAN, if the number of dynamic mac and the number of mac in the VLAN is larger than the max number allowed, users will see debug information.” no debug vlan mac count” command is used to disable the number limitation function debug of mac in the VLAN.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic mac in the VLAN.

Examples：

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current mac count 21 is more than or equal to the maximum limit in vlan 1!!
%Jun 14 16:04:40 2007 Mac learning will be stopped and some mac will be delete !!
```

6.3.15 debug ip arp count

Command：debug ip arp count

no debug ip arp count

Function：When the number limitation function debug of arp in the VLAN, if the number of dynamic arp and the number of arp in the VLAN is larger than the max number allowed, users will see debug information.” no debug ip arp count” command is used to disable the number limitation function debug of arp in the VLAN.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic arp in the VLAN.

Examples：

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current arp count 21 is more than or equal to the maximum limit in vlan 1!!
%Jun 14 16:04:40 2007Arp learning will be stopped and some arp will be delete !!
```

6.3.16 debug ipv6 nd count

Command：debug ipv6 nd count

no debug ipv6 nd count

Function：When the number limitation function debug of neighbor in the VLAN, if the number of dynamic neighbor and the number of neighbor in the VLAN is larger than the max number allowed, users will see debug information.” no debug ip neighbor count” command is used to disable the number limitation function debug of neighbor in the VLAN.

Parameters：None

Command Mode：Admin Mode

Default Settings：None

Usage Guide：Display the debug information of the number of dynamic neighbor in the VLAN.

Examples：

```
Switch#debug vlan mac count
%Jun 14 16:04:40 2007 Current neighbor count 21 is more than or equal to the maximum limit in
vlan 1!!
%Jun 14 16:04:40 2007Neighbor learning will be stopped and some neighbor will be delete !!
```

6.4 The Number Limitation Function of Port, MAC in VLAN and IP Example

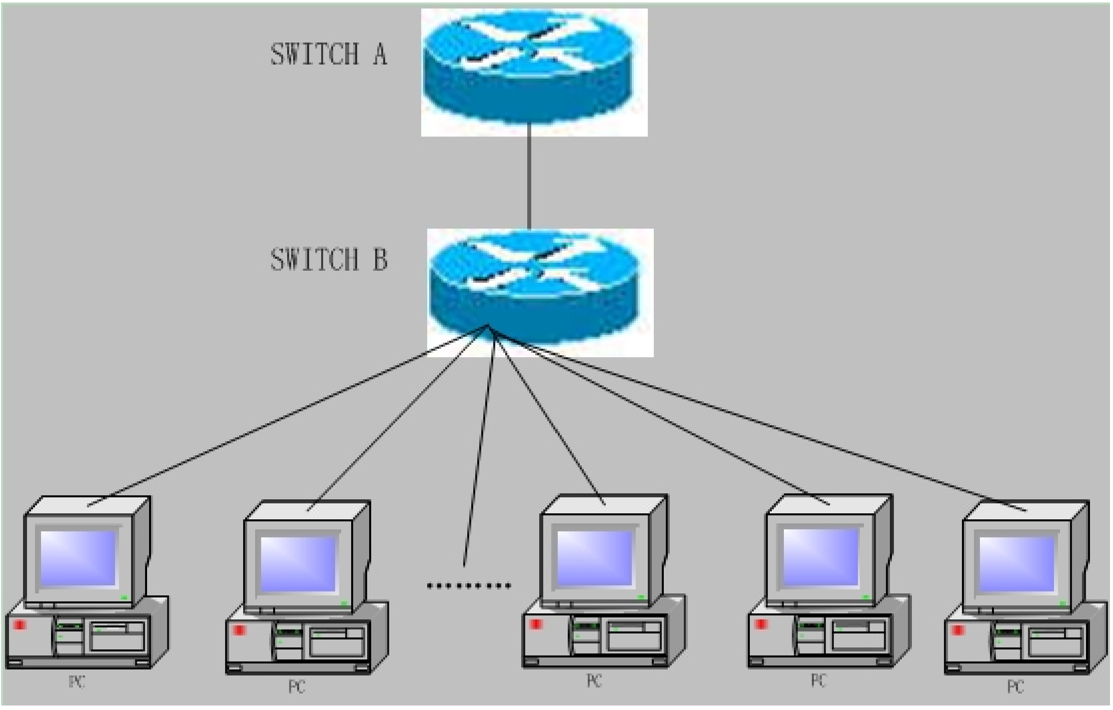


Fig 6-1 The Number Limitation of Port, MAC in VLAN and IP Typical Configuration Example

In the network topology above, SWITCH B connects to many PC users, before enabling the number limitation function of port, MAC in VLAN and IP, if the system hardware has no other limitation, SWTICH A and SWTICH B can get the MAC, ARP, ND list entries of all the PC, so limiting the MAC, ARP list entry can avoid DOS attack to a certain extent. When malicious users frequently do MAC or ARP cheating, it will be easy for them to fill the MAC and ARP list entries of the switch, causing successful DOS attacks. Limiting the MAC, ARP list entry can prevent DOS attack.

On port 3/1 of SWITCH A, set the max number can be learnt of dynamic MAC address as 20, of dynamic ARP address as 20, NEIGHBOR list entry as 10. In VLAN 1, set the max number of dynamic MAC address as 30, of dynamic ARP address as 30, NEIGHBOR list entry as 20.

SWITCH A configuration task sequence:

```
Switch(config)#
Switch (config)#int ethernet 3/1
Switch (Config-If-Ethernet3/1)#switchport mac-address dynamic maximum 20
Switch (Config-If-Ethernet3/1)#switchport arp dynamic maximum 20
Switch (Config-If-Ethernet3/1)#switchport nd dynamic maximum 10
Switch (Config-if-Vlan1)#vlan mac-address dynamic maximum 30
Switch (Config-if-Vlan1)#ip arp dynamic maximum 30
Switch (Config-if-Vlan1)#ipv6 nd dynamic maximum 20
```

6.5 The Number Limitation Function Of Port, MAC in VLAN and IP Troubleshooting Help

The number limitation function of port, MAC in VLAN and IP is disabled by default, if users need to limit the number of user accessing the network, they can enable it. If the number limitation function of MAC address can not be configured, please check whether Spanning-tree, dot1x, TRUNK is running on the switch and whether the port is configured as a MAC-binding port. The number limitation function of MAC address is mutually exclusive to these configurations, so if the users need to enable the number limitation function of MAC address on the port, they should check these functions mentioned above on this port are disabled.

If all the configurations are normal, after enabling the number limitation function of port, MAC in VLAN and IP, users can use debug commands to debug every limitation, check the details of number limitations and judge whether the number limitation function is correct. If there is any problem, please sent result to technical service center.

Chapter 7 Operational Configuration of AM Function

7.1 Introduction to AM Function

AM (Access Management) means that when a switch receives an IP or ARP message, it will compare the information extracted from the message (such as source IP address or source MAC-IP address) with the configured hardware address pool. If there is an entry in the address pool matching the information (source IP address or source MAC-IP address), the message will be forwarded, otherwise, dumped. The reason why source-IP-based AM should be supplemented by source-MAC-IP-based AM is that IP address of a host might change. Only with a bound IP, can users change the IP of the host into forwarding IP, and hence enable the messages from the host to be forwarded by the switch. Given the fact that MAC-IP can be exclusively bound with a host, it is necessary to make MAC-IP bound with a host for the purpose of preventing users from maliciously modifying host IP to forward the messages from their hosts via the switch.

With the interface-bound attribute of AM, network mangers can bind the IP (MAC-IP) address of a legal user to a specified interface. After that, only the messages sending by users with specified IP (MAC-IP) addresses can be forwarded via the interface, and thus strengthen the monitoring of the network security.

7.2 AM Function Configuration Task List

1. Enable AM function
2. Enable AM function on an interface
3. Configure the forwarding IP
4. Configure the forwarding MAC-IP
5. Delete all of the configured IP or MAC-IP or both
6. Display relative configuration information of AM

1. Enable AM function

Command	Explanation
Global Mode	
am enable **no am enable**	Globally enable or disable AM function.

2. Enable AM function on an interface

Command	Explanation

Interface Mode	
am interface **no am interface**	Enable/disable AM function on the interface. When the AM function is enabled on the interface, no IP or ARP message will be forwarded by default.

3.Configure the forwarding IP

Command	Explanation
Interface Mode	
am ip-pool <*ip-address*> <*num*> **no am ip-pool <*ip-address*> <*num*>**	Configure the forwarding IP of the interface.

4. Configure the forwarding MAC-IP

Command	Explanation
Interface Mode	
am mac-ip-pool <*mac-address*> <*ip-address*> **no am mac-ip-pool <*mac-address*> <*ip-address*>**	Configure the forwarding MAC-IP of the interface.

5. Delete all of the configured IP or MAC-IP or both

Command	Explanation
Global Mode	
no am all [ip-pool|mac-ip-pool]	Delete MAC-IP address pool or IP address pool or both pools configured by all users.

6. Display relative configuration information of AM

Command	Explanation
Admin Mode	
show am [interface <*interface-name*>]	Display the AM configuration information of one interface or all interfaces.

7.3 Command for AM Configuration

7.3.1 am enable

Command：am enable

no am enable

Function：Globally enable/disable AM function.

Parameters：None.

Default：AM function is disabled by default.

Command Mode：Global Mode.

Usage Guide：None.

Example：Enable AM function on the switch.

```
Switch(config)#am enable
```

Disable AM function on the switch.

```
Switch(config)#no am enable
```

7.3.2 am interface

Command：am interface

no am interface

Function：Enable/disable AM function on an interface.

Parameters：None.

Default：AM function is disabled on all interfaces.

Command Mode：Interface Mode.

Example：Enable AM function on interface 2/3 of the switch.

```
Switch(Config-If-Ethernet 2/3)#am interface
```

Disable AM function on interface 2/3 of the switch.

```
Switch(Config-If-Ethernet 2/3)#no am interface
```

7.3.3 am ip-pool

Command：am ip-pool <*ip-address*> <*num*>

no am ip-pool <*ip-address*> <*num*>

Function：Set the AM IP segment of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

Parameters：<*ip-address*> the starting address of an address segment in the IP address pool; **<*num*>** is the number of consecutive addresses following ip-address, less than or equal with 32.

Default：IP address pool is empty.

Command Mode：Interface Mode.

Usage Guide：None.

Example：Configure that interface 2/3 of the switch will forward data packets from an IP address which is one of 10 consecutive IP addresses starting from 10.10.10.1

```
Switch(Config-If-Ethernet 2/3)#am ip-pool 10.10.10.1 10
```

7.3.4 am mac-ip-pool

Command：am mac-ip-pool <*mac-address*> < *ip-address*>

no am mac-ip-pool <*mac-address*> < *ip-address*>

Function：Set the AM MAC-IP address of the interface, allow/deny the IP messages or APR messages from a source IP within that segment to be forwarded via the interface.

Parameter：<*mac-address*> is the source MAC address; **< *ip-address*>** is the source IP address of the packets, which is a 32 bit binary number represented in four decimal numbers.

Default：MAC-IP address pool is empty.

Command Mode：Interface Mode.

Usage Guide：None.

Example：Configure that the interface 2/3 of the switch will allow data packets with a source MAC address of 11-22-22-11-11-11 and a source IP address of 10.10.10.1 to be forwarded.

```
Switch(Config-If-Ethernet2/3)#am mac-ip-pool 11-22-22-11-11-11 10.10.10.1
```

Special Explanation：when there are both cards support IPV6 and those not, some FFP rules will be added to the gigabit interfaces not support IPV6 to deal with IPv6 proxy and protocol messages and thus take up some FFP resources. And as a result, AM function can only be partly enabled (limited by hardware resources), and am ip-pool or am mac-ip-pool are mutually exclusive.

7.3.5 no am all

Command：no am all [ip-pool | mac-ip-pool]

Function：Delete MAC-IP address pool or IP address pool or both pools configured by all users.

Parameters：ip-pool is the IP address pool; **mac-ip-pool** is the MAC-IP address pool; no parameter means both address pools.

Default：Both address pools are empty at the beginning.

Command Mode：Global Mode

Usage Guide：None.

Example：Delete all configured IP address pools.

```
Switch(config)#no am all ip-pool
```

7.3.6 show am

Command：show am [interface <*interface-name*>]

Function：Display the configured AM entries.

Parameters：<*interface-name*> is the name of the interface of which the configuration information will be displayed. No parameter means to display the AM configuration information of all interfaces.

Command Mode：Admin Mode.

Example：Display all configured AM entries.

```
Switch#show am
AM is enabled

Interface Ethernet1/3
          am interface
          am ip-pool 30.10.10.1   20
Interface Ethernet1/5
          am interface
          am ip-pool 50.10.10.1   30
          am mac-ip-pool   00-02-04-06-08-09 20.10.10.5
          am ip-pool 50.20.10.1   20
Interface Ethernet1/6
          am interface
Interface Ethernet1/1
          am interface
          am ip-pool 10.10.10.1   20
          am ip-pool 10.20.10.1   20
```

Display the AM configuration entries of ehternet/5 of the switch.

```
Switch#show am interface ethernet 1/5
AM is enabled

Interface Etherne1/5
          am interface
          am ip-pool 50.10.10.1   30
          am mac-ip-pool   00-02-04-06-08-09 20.10.10.5
     am ip-pool 50.20.10.1   20
```

7.4 Example of AM Function

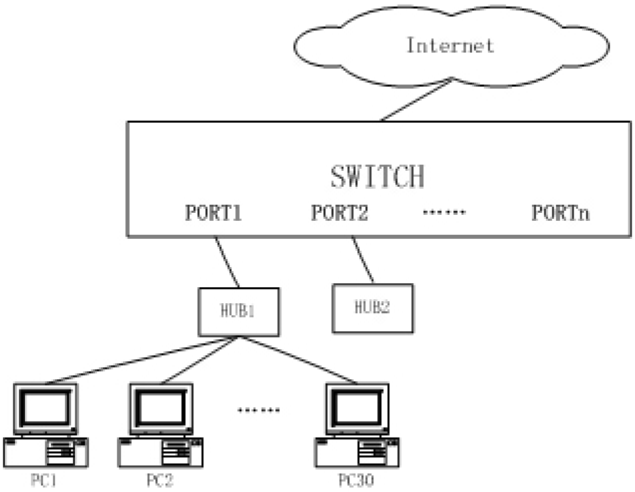


Fig 7-1 a typical configuration example of AM function

In the topology above, 30 PCs, after converged by HUB1, connect with interface1 on the switch. The IP addresses of these 30 PCs range from 100.10.10.1 to 100.10.10.30. Considering security, the system manager will only take user with an IP address within that range as legal ones. And the switch will only forward data packets from legal users while dumping packets from other users.

According to the requirements mentioned above, the switch can be configured as follows:

```
Switch(config)#am enable
Switch(config)#interface ethernet1/1
Switch(Config-If-Ethernet1/1)#am interface
Switch(Config-If-Ethernet1/1)#am ip-pool 10.10.10.1 10
```

7.5 AM Function Troubleshooting

AM function is disabled by default, and after it is enabled, relative configuration of AM can be made.

Users can view the current AM configuration with “show am” command, such as whether the AM is enabled or not, and AM information on each interface, they can also use “show am [interface <*interface-name*>]” command to check the AM configuration information on a specific interface.

If any operational error happens, the system will display detailed corresponding prompt.

Chapter 8 Security Feature Configuration

8.1 Security Feature Introduction

Before introducing the security features, we here first introduce the DoS. The DoS is short for Denial of Service, which is a simple but effective destructive attack on the internet. The server under DoS attack will drop normal user data packet due to non-stop processing the attacker’s data packet, leading to the denial of the service and worse can lead to leak of sensitive data of the server.

Security feature refers to applications such as protocol check which is for protecting the server from attacks such as DoS. The protocol check allows the user to drop matched packets based on specified conditions. The security features provide several simple and effective protections against Dos attacks while acting no influence on the linear forwarding performance of the switch.

8.2 Security Feature Configuration

8.2.1 Prevent IP Spoofing Function Configuration Task Sequence

1. Enable the IP spoofing function.

Command	Explanation
Global Mode	
[no] dosattack-check srcip-equal-dstip enable	Enable/disable the function of checking if the IP source address is the same as the destination address

8.2.2 Prevent TCP Unauthorized Label Attack Function Configuration Task List

1. Enable the anti TCP unauthorized label attack function
2. Enable Checking IPv4 fragment function

Command	Explanation
Global Mode	
[no] dosattack-check tcp-flags enable	Enable/disable checking TCP label function
[no] dosattack-check ipv4-first-fragment enable	Enable/disable checking IPv4 fragment. This command has no effect when used separately, but if this function is not enabled, the switch will not drop the IPv4 fragment packet containing unauthorized TCP labels

8.2.3 Anti Port Cheat Function Configuration Task Sequence

1．Enable the anti port cheat function

Command	Explanation
Global Mode	
[no] dosattack-check srcport-equal-dstport enable	Enable/disable the prevent-port-cheat function

8.2.4 Prevent TCP Fragment Attack Function Configuration Task Sequence

1．Enable the prevent TCP fragment attack function

2．Configure the minimum permitted TCP head length of the packet

Command	Explanation
Global Mode	
[no] dosattack-check tcp-fragment enable	Enable/disable the prevent TCP fragment attack function
dosattack-check tcp-header <*size*>	**dosattack-check tcp-fragment enable** Configure the minimum permitted TCP head length of the packet. This command has no effect when used separately, the user should enable the **dosattack-check tcp-fragment enable**

8.2.5 Prevent ICMP Fragment Attack Function Configuration Task Sequence

1．Enable the prevent ICMP fragment attack function

2．Configure the max permitted ICMPv4 net load length

3．Configure the max permitted ICMPv6 net load length

Command	Explanation
Global Mode	
[no] dosattack-check icmp-attacking enable	Enable/disable the prevent ICMP fragment attack function
dosattack-check icmpv4-size <*size*>	Configure the max permitted ICMPv4 net length. This command has not effect when used separately, the user have to enable the **dosattack-check icmp-attacking enable**

dosattack-check icmpv6-size <*size*>	Configure the max permitted ICMPv6 net length. This command has not effect when used separately, the user have to enable the **dosattack-check icmp-attacking enable**

8.3 Commands for Security Feature

8.3.1 dosattack-check srcip-equal-dstip enable

Command: [no] dosattack-check srcip-equal-dstip enable

Function: Enable the function by which the switch checks if the source IP address is equal to the destination IP address; the "no" form of this command disables this function.

Parameter: None

Default: Disable the function by which the switch checks if the source IP address is equal to the destination IP address.

Command Mode: Global Mode

Usage Guide: By enabling this function, data packet whose source IP address is equal to its destination address will be dropped

Example: Drop the data packet whose source IP address is equal to its destination address

```
Switch(config)# dosattack-check srcip-equal-dstip enable
```

8.3.2 dosattack-check ipv4-first-fragment enable

Command: [no] dosattack-check ipv4-first-fragment enable

Function: Enable the function by which the switch checks the first fragment packet of IPv4; the "no" form of this command disables this function.

Parameter: None

Command Mode: Global Mode

Usage Guide: This command has no effect when used separately. It should be used associating **dosattack-check tcp-flags enable** or **dosattack-check srcport-equal-dstport enable** command.

Example: Drop the IPv4 fragment or non-fragment data packet whose source port is equal to its destination port.

```
Switch(config)# dosattack-check ipv4-first-fragment enable
Switch(config)# dosattack-check srcport-equal-dstport enable
```

8.3.3 dosattack-check tcp-flags enable

Command: [no] dosattack-check tcp-flags enable

Function: Enable the function by which the switch will check the unauthorized TCP label function;

the “no” form of this command will disable this function.

Parameter: None

Default: This function disable on the switch by default

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop follow four data packets containing unauthorized TCP label: SYN=1 while source port is smaller than 1024;TCP label positions are all 0 while its serial No. =0;FIN=1,URG=1,PSH=1 and the TCP serial No.=0;SYN=1 and FIN=1. This function can be used associating the “dosattack-check ipv4-first-fragment enable” command

Example: Drop one or more types of above four packet types.

```
Switch(config)# dosattack-check tcp-flags enable
```

8.3.4 dosattack-check srcport-equal-dstport enable

Command: [no] dosattack-check srcport-equal-dstport enable

Function: Enable the function by which the switch will check if the source port is equal to the destination port; the "no" form of this command disables this function

Parameter: None

Default: Disable the function by which the switch will check if the source port is equal to the destination port

Command Mode: Global Mode

Usage Guide: With this function enabled, the switch will be able to drop TCP and UDP data packet whose destination port is equal to the source port. This function can be used associating the “dosattack-check ipv4-first-fragment enable” function so to block the IPv4 fragment TCP and UDP data packet whose destination port is equal to the source port

Example: Drop the non-fragment TCP and UDP data packet whose destination port is equal to the source port

```
Switch(config)#dosattack-check srcport-equal-dstport enable
```

8.3.5 dosattack-check tcp-fragment enable

Command: [no] dosattack-check tcp-fragment enable

Function: Enable the function by which the switch detects TCP fragment attacks; the “no” form of this command disables this function

Parameter: None

Default: This function is not enabled on the switch by default

Command Mode: Global Mode

Usage Guide: By enabling this function the switch will be protected from the TCP fragment attacks, dropping the data packets whose TCP fragment offset value is 1 or the TCP head is shorter than the specified value. Use “dosattack-check tcp-header” command to specify the length.

Example: Enable the Checking TCP fragment attack function.

```
Switch(config)# dosattack-check tcp-fragment enable
```

8.3.6 dosattack-check tcp-header

Command: dosattack-check tcp-header <size>

Function: Configure the minimum TCP head length permitted by the switch

Parameter: <size> is the minimum TCP head length permitted by the switch

Default: The length is 20 by default which is the shortest TCP head

Command Mode: Global Mode

Usage Guide: To use this function the "dosattack-check tcp-fragment enable" function must be enabled

Example: Set the minimum TCP head length permitted by the switch to 20

```
Switch(config)# dosattack-check tcp-fragment enable
Switch(config)# dosattack-check tcp-header 20
```

8.3.7 dosattack-check icmp-attacking enable

Command: [no] dosattack-check icmp-attacking enable

Function: Enable the ICMP fragment attack checking function on the switch; the "no" form of this command disables this function

Parameter: None

Default: Disable the ICMP fragment attack checking function on the switch

Command Mode: Global Mode

Usage Guide: With this function enabled the switch will be protected from the ICMP fragment attacks, dropping the fragment ICMPv4/v6 data packets whose net length is smaller than the specified value

Example: Enable the ICMP fragment attack checking function

```
Switch(config)# dosattack-check icmp-attacking enable
```

8.3.8 dosattack-check icmpv4-size

Command: dosattack-check icmpv4-size <size>

Function: Configure the max net length of the ICMPv4 data packet permitted by the switch

Parameter: <size> is the max net length of the ICMPv4 data packet permitted by the switch

Default: The value is 0x200 by default

Command Mode: Global Mode

Usage Guide: To use this function you have to enable "dosattack-check icmp-attacking enable" first

Example: Set the max net length of the ICMPv4 data packet permitted by the switch to 100

```
Switch(config)# dosattack-check icmp-attacking enable
Switch(config)# dosattack-check icmpv4-size 100
```

8.3.9 dosattack-check icmpv6-size

Command:dosattack-check icmpv6-size <size>

Function: Configure the max net length of the ICMPv6 data packet permitted by the switch

Parameter:<size> is the max net length of the ICMPv6 data packet permitted by the switch

Default: The value is 0x200 by default

Command Mode: Global Mode

Usage Guide: To use this function you have to enable "dosattack-check icmp-attacking enable" first

Example: Set the max net length of the ICMPv6 data packet permitted by the switch to 100

```
Switch(config)# dosattack-check icmp-attacking enable
Switch(config)# dosattack-check icmpv6-size 100
```

8.4 Security Feature Example

Scenario:

The User has follows configuration requirements: the switch do not forward data packet whose source IP address is equal to the destination address, and those whose source port is equal to the destination port. Only the ping command with defaulted options is allowed within the IPv4 network, namely the ICMP request packet can not be fragmented and its net length is normally smaller than 100

Configuration procedure:

```
Switch(config)# dosattack-check srcip-equal-dstip enable
Switch(config)# dosattack-check srcport-equal-dstport enable
Switch(config)# dosattack-check ipv4-first-fragment enable
Switch(config)# dosattack-check icmp-attacking enable
Switch(config)# dosattack-check icmpv4-size 100
```

Chapter 9 SSL Configuration

9.1 SSL Introduction

As the computer networking technology spreads, the security of the network has been taking more and more important impact on the availability and the usability of the networking application. The network security has become one of the greatest barrier of modern networking applications.

To protect sensitive data transferred through Web, Netscape introduced the Secure Socket Layer – SSL protocol, for its Web browser. Up till now, SSL 2.0 and 3.0 has been released. SSL 2.0 is obsolete because of security problems, and it is not supported on the switches of Digital China Network. The SSL protocol uses the public-key encryption, and has become the industry standard for secure communication on internet for Web browsing.

SSL is a safety protocol to protect private data transmission on the Internet. SSL protocols are designed for secure transmission between the client and the server, and authentication both at the server sides and optional client. SSL protocols must build on reliable transport layer (such as TCP). SSL protocols are independent for application layer. Some protocols such as HTTP, FTP, TELNET and so on, can build on SSL protocols transparently. The SSL protocol negotiates for the encryption algorithm, the encryption key and the server authentication before data is transmitted. Ever since the negotiation is done, all the data being transferred will be encrypted.

Via above introduction, the security channel provided by SSL protocols have below three chatacteristics:

- ☞ Privacy. First they encrypt the suite through negotiation, then all the messages be encrypted.
- ☞ Affirmation. Though the client authentication of the conversational is optional, but the server is always authenticated.
- ☞ Reliability. The message integrality inspect is included in the sending message (use MAC).

9.1.1 Basic Element of SSL

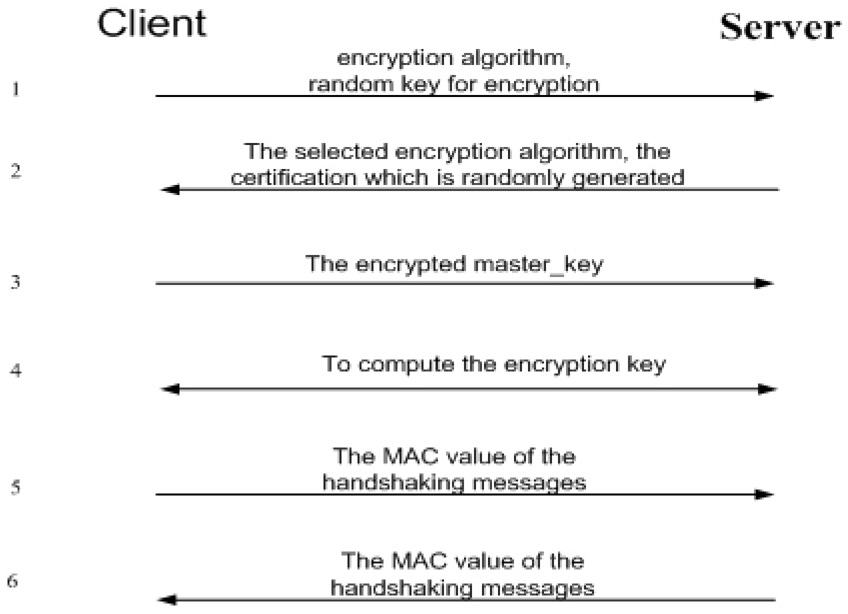
The basic strategy of SSL provides a safety channel for random application data forwarding between two communication programs. In theory, SSL connect is similar with encrypt TCP connect. The position of SSL protocol is under application layer and on the TCP. If the mechanism of the data forwarding in the lower layer is reliable, the data read-in the network will be forwarded to the other program in sequence, lose packet and re-forwarding will not appear. A lot of transmission protocols can provide such kind of service in theory, but in actual application, SSL is almost running on TCP, and not running on UDP and IP directly.

When web function is running on the switch and client visit our web site through the internet browser, we can use SSL function. The communication between client and switch through SSL connect can improve the security.

Firstly, SSL should be enabled on the switch. When the client tries to access the switch through https method, a SSL session will be set up between the switch and the client. When the SSL session has been set up, all the data transmission in the application layer will be encrypted.

SSH handshake is done when the SSL session is being set up. The switch should be able to provide certification keys. Currently the keys provided by the switch are not the formal certification keys issued by official authurities, but the private certification keys generated by ssh software under linux which may not be recognized by the web browser. With regard to the switch application, it is not necessary to apply for a formal SSL certification key. A private certification key is enough to make the communication safe between the users and the switch. Currently it is not required that the client is able to check the validation of the certification key. The encryption key and the encryption method should be negotiated during the handshake period of the session which will be then used for data encryption.

SSL session handshake process:


Client
Server
1
encryption algorithm, random key for encryption
2
The selected encryption algorithm, the certification which is randomly generated
3
The encrypted master_key
4
To compute the encryption key
5
The MAC value of the handshaking messages
6
The MAC value of the handshaking messages

9.2 SSL Configuration task list

1. Enable/disable SSL function (need)
2. Configure/delete port number by SSL used (optional)
3. Configure/delete secure cipher suite by SSL used (optional)
4. Maintenance and diagnose for the SSL function (optional)

1. Enable/disable SSL function

Command	Explanation
Global Mode	
ip http secure-server **no ip http secure-server**	Enable/disable SSL function

2. Configure/delete port number by SSL used

Command	Explanation
Global Mode	
ip http secure-port ***<port-number>*** **no ip http secure-port**	Configure/delete port number by SSL used, the **no ip http secure-port** command deletes theport number.

3. Configure/delete secure cipher suite by SSL used

Command	Explanation
Global Mode	
ip http secure-ciphersuite {des-cbc3-sha|rc4-128-sha| des-cbc-sha} **no ip http secure-ciphersuite**	Configure/delete secure cipher suite by SSL used

4. Maintenance and diagnose for the SSL function

Command	Explanation
Admin Mode or Configuration Mode	
show ip http secure-server status	Show the configured SSL information.
debug ssl **no debug ssl**	Open/close the DEBUG for SSL function.

9.3 SSL Configuration Command

9.3.1 ip http secure-server

Command：ip http secure-server

no ip http secure-server

Function: Enable/disable SSL function.

Parameter: None.

Command Mode: Global Mode.

Default: Disabled.

Usage Guide: This command is used for enable and disable SSL function. After enable SSL function, the users visit the switch through https client, switch and client use SSL connect, can form safety SSL connect channel. After that, all the data which transmit of the application layer will be encrypted, then ensure the privacy of the communication.

Example: Enable SSL function.

```
Switch(config)#ip http secure-server
```

9.3.2 ip http secure-port

Command：ip http secure-port <*port-number*>

no ip http secure-port

Function: Configure/delete port number by SSL used.

Parameter: ***<port-number>*** means configured port number, range between 1025 to65525. 443 is for default.

Command Mode: Global Mode.

Default: Not configure.

Usage Guide: If this command is used to configure the port number, then the configured port number is used to monitor. If the port number for https is changed, when users try to use https to connect, must use the changed one. For example: https://device:port_number. SSL function must reboot after every change.

Example: Configure the port number is 1028

```
Switch(config)#ip http secure-port 1028
```

9.3.3 ip http secure- ciphersuite

Command：ip http secure-ciphersuite {des-cbc3-sha|rc4-128-sha| des-cbc-sha}

no ip http secure-ciphersuite

Function: Configure/delete secure cipher suite by SSL used.

Parameter: des-cbc3-sha encrypted algorithm DES_CBC3，summary algorithm SHA.

rc4-128-sha encrypted algorithm RC4_128，summary algorithm SHA.

des-cbc-sha encrypted algorithm DES_CBC，summary algorithm SHA.

default use is rc4-md5.

Command Mode: Global Mode.

Default: Not configure.

Usage Guide: If this command is used to configure the secure cipher suite, specified encryption method will be used. The SSL should be restarted to take effect after changes on configuration. When des-cbc-sha is configured, IE 7.0 or above is required.

Example: Configure the secure cipher suite is rc4-128-sha.

```
Switch(config)#ip http secure- ciphersuite rc4-128-sha
```

9.3.4 show ip http secure-server status

Command：show ip http secure-server status

Parameter: Show the status for the configured SSL.

Parameter: None.

Command Mode: Admin Mode or Configuration Mode.

Example：

```
Switch# show ip http secure-server status
HTTP secure server status: Enabled
HTTP secure server port: 1028
HTTP secure server ciphersuite: rc4-128-sha
```

9.3.5 debug ssl

Command：debug dns ssl
no debug ssl

Function: Show the configured SSL information, the no form close the DEBUG.

Parameter: None.

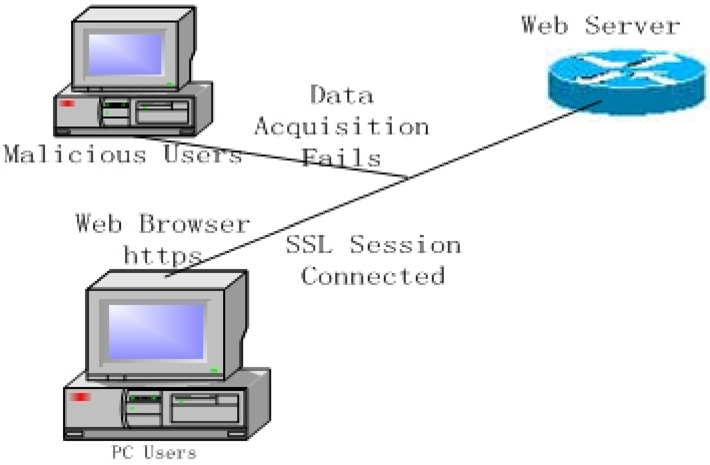
Command Mode: Admin Mode.

Example：

```
Switch#debug ssl
%Jan 01 01:02:05 2006 ssl will to connect to web server 127.0.0.1:9998
%Jan 01 01:02:05 2006 connect to http security server sucess!
```

9.4 SSL Typical Example

When the web function is enabled on the switch, SSH can be configured for users to access the web interface on the switch. If the SSL has been configured, communication between the client and the switch will be encrypted through SSL for safety.



Configuration on the switch：

```
Switch(config)#ip http secure-server
Switch(config)#ip http secure-port 1025
Switch(config)#ip http secure-ciphersuite rc4-128-sha
```

9.5 SSL Troubleshooting

In configuring and using SSL, the SSL function may fail due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ✧ First good condition of the physical connection;
- ✧ Second all interface and link protocols are in the UP state (use “show interface” command)
- ✧ Then, make sure SSL function is enabled (use ip http secure-server command);
- ✧ Don’t use default port number if configured port number, pay attention to the port number when input the webwite.
- ✧ If SSL is enabled, SSL should be restarted after changes is taked on the port configuration and encryption configuration.
- ✧ IE 7.0 or above should be used for use of des-cbc-sha

Chapter 10 IPv6 Security RA Configuration

10.1 IPv6 Security RA Introduction

In IPv6 networks, the network topology is generally compromised of routers, layer-two switches and IPv6 hosts. Routers usually advertise RA, including link prefix, link MTU and other information, when the IPv6 hosts receive RA, they will create link address, and set the default router as the one sending RA in order to implement IPv6 network communication. If a vicious IPv6 host sends RA to cause that normal IPv6 users set the default router as the vicious IPv6 host user, the vicious user will be able to capture the information of other users, which will threat the network security. Simultaneously, the normal users get incorrect address and will not be able to connect to the network. So, in order to implement the security RA function, configuring on the switch ports to reject vicious RA messages is necessary, thus to prevent forwarding vicious RA to a certain extent and to avoid affecting the normal operation of the network.

10.2 IPv6 Security RA Configuration Task List

1. Globally enable IPv6 security RA
2. Enable IPv6 security RA on a port
3. Display and debug the relative information of IPv6 security RA

1. Globally enable IPv6 security RA

Command	Explanation
Global configuration mode	
ipv6 security-ra enable **no ipv6 security-ra enable**	Globally enable and disable IPv6 security RA.

2. Enable IPv6 security RA on a port

Command	Explanation
Port configuration mode	
ipv6 security-ra enable **no ipv6 security-ra enable**	Enable and disable IPv6 security RA in port configuration mode.

3. Display and debug the relative information of IPv6 security RA

Command	Explanation
Admin mode	

debug ipv6 security-ra **no debug ipv6 security-ra**	Enable the debug information of IPv6 security RA module, the no operation of this command will disable the output of debug information of IPv6 security RA.
show ipv6 security-ra [interface <*interface-list*>]	Display the untrust ports and whether globally security RA is enabled.

10.3 IPv6 Security RA Commands

10.3.1 ipv6 security-ra enable

Command：ipv6 security-ra enable

no ipv6 security-ra enable

Function：Globally enable IPv6 security RA function, all the RA advertisement messages will not be forwarded through hardware, but only sent to CPU to handle. The no operation of this command will globally disable IPv6 security RA function.

Parameters：None.

Command Mode：Global configuration mode.

Default：The IPv6 security RA function is disabled by default.

Usage Guide：Only after globally enabling the security RP function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.

Example：Globally enable IPv6 security RA.

```
Switch(config)#ipv6 security-ra enable
```

10.3.2 ipv6 security-ra enable

Command：ipv6 security-ra enable

no ipv6 security-ra enable

Function：Enable IPv6 security RA on a port , causing this port not to forward the received RA message. The **no ipv6 security-ra enable** will disable the IPv6 security RA on a port.

Parameters：None.

Command Mode：Port configuration mode.

Default：IPv6 security RA function is disabled by default.

Usage Guide：Only after globally enabling the security RP function, can the security RA on a port be enabled. Globally disabling security RA will clear all the configured security RA ports.

Example：Enable IPv6 security RA on a port.

```
Switch(Config-If-Ethernet1/2)#ipv6 security-ra enable
```

10.3.3 show ipv6 security-ra

Command：**show ipv6 security-ra [interface <*interface-list*>]**

Function：Display all the interfaces with ipv6 urpf function enabled.

Parameters：No parameter will display all the untrust ports, entering a parameter will display the corresponding untrust port.

Command Mode：Admin mode.

Example：

```
Switch#show ipv6 security-ra
IPv6 security ra config and state information in the switch
Global IPv6 Security RA State: Enable
Ethernet1/1
IPv6 Security RA State: Yes
Ethernet1/3
IPv6 Security RA State: Yes
```

10.3.4 debug ipv6 security-ra

Command：**debug ipv6 security-ra**

no debug ipv6 security-ra

Function：Enable the debug information of IPv6 security RA; the no operation of this command will disable the debug information of IPv6 security RA.

Command Mode：Admin mode.

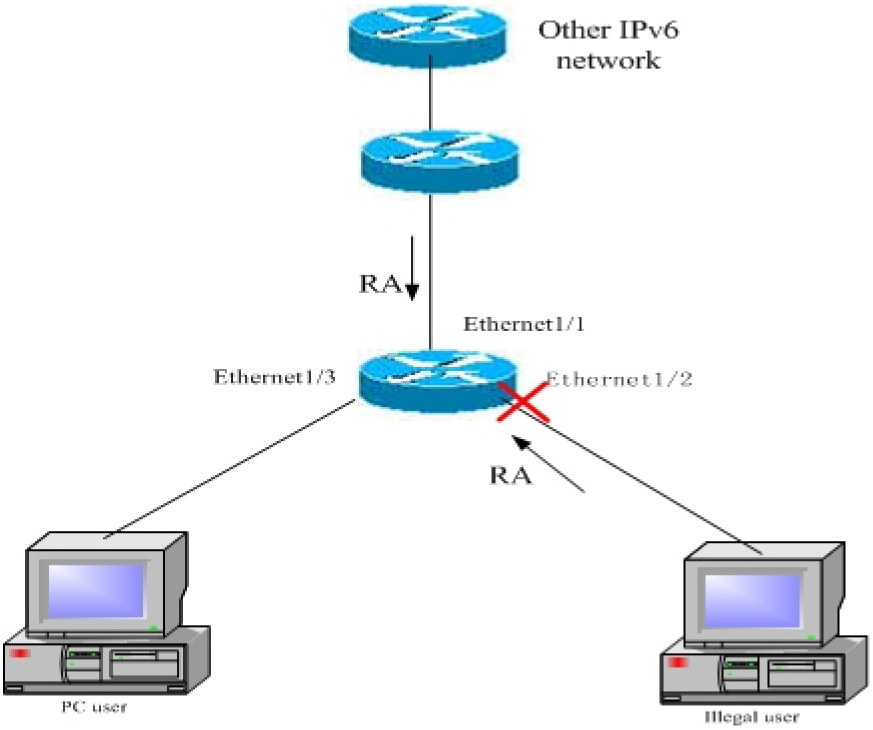
Parameters：None.

Usage Guide：Users can check the proceeds of message handling of IPv6 security RA, which will help investigate the causes to problems if there is any.

Example：Enable the debug information of IPv6 security RA.

```
Switch#debug ipv6 security-ra
```

10.4 IPv6 Security RA Typical Examples



Instructions: if the illegal user in the graph advertises RA, the normal user will receive the RA, set the default router as the vicious IPv6 host user and change its own address. This will cause the normal user to not be able to connect the network. We want to set security RA on the 1/2 port of the switch, so that the RA from the illegal user will not affect the normal user.

Switch configuration task sequence:

```
Switch#config
Switch(config)#ipv6 security-ra enable
Switch(Config-If-Ethernet1/2)#ipv6 security-ra enable
```

10.5 IPv6 Security RA Troubleshooting Help

The function of IPv6 security RA is quite simple, if the function does not meet the expectation after configuring IPv6 security RA:

- ✧ Check if the switch is correctly configured.
- ✧ Check if there are rules conflicting with security RA function configured on the switch, this kind of rules will cause RA messages to be forwarded.
- ✧ If the configuration is correct, but the operation of security RA still dose not meet the expectations, please enable the debug function of security RA, and send the result to the technology service center.