Content

Chapter 1 ACL Configuration

1.1 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.

1.1.1 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.

1.1.2 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.

1.1.3 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.

1.2 ACL Configuration Task List

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 MAC 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 IPv6 access-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 an incoming direction of the specified port

5. Clear the filtering information of the specified port

1. Configuring access-list

(1) Configuring a numbered standard IP access-list

Command	Explanation
Global Mode	
access-list <*num*> {deny | permit} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} **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 {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*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 {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*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 {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [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 {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [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*>} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [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	
ip access-list standard <*name*> **no ip access-list standard <*name*>**	Creates a standard IP access-list based on nomenclature; the "**no ip access-list standard <*name*>**" command deletes the name-based standard IP access-list.

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

Command	Explanation
Standard IP ACL Mode	
[no] {deny | permit} {{<*slpAddr*> <*slMask*>} | any-source | {host-source <*slpAddr*>}}	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	
ip access-list extended <*name*> **no ip access-list extended <*name*>**	Creates an extended IP access-list basing on nomenclature; the "**no ip access-list 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 {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*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 {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [<*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 {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [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 {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} [s-port {<*sPort*> | range <*sPortMin*> <*sPortMax*>}] {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [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>} {{<*slpAddr*> <*sMask*>} | any-source | {host-source <*slpAddr*>}} {{<*dlpAddr*> <*dMask*>} | any-destination | {host-destination <*dlpAddr*>}} [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 an extensive MAC 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*>]]	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*>}} [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]]]	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 name-based extended MAC access rule matching 802.3 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*>}}[tagged-eth2 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]] [ethertype<*protocol*> [<*protocol-mask*>]]]	Creates an name-based extended MAC access rule matching tagged 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*>}} [tagged-802-3 [cos <*cos-val*> [<*cos-bitmask*>]] [vlanId <*vid-value*> [<*vid-mask*>]]]	Creates an name-based extended MAC access rule matching tagged 802.3 frame; the no form command deletes this name-based extended 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-ip 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-*	Creates a numbered mac-udp extended mac-ip

***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 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 numbered extended MAC-IP access rule.

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

a. Create an 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 <*dPortMin*> <*dPortMax*>}] [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-	Creates an extended

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*>]	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 <*slpv6Addr*>}} **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 IPv6 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 <*fl*>][time-range<*time-range-name*>] **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*>][time-range<*time-range-name*>]** **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*>][time-range<*time-range-name*>]** **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 <*fl*>][time-range<*time-range-name*>]** **no ipv6 access-list <*num*>**	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 command deletes a numbered standard IPv6 access-list.

（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 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 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*>} |	Creates an extended name-based ICMP IPv6 access rule; the no form command deletes

any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [<*icmp-type*> [<*icmp-code*>]] [dscp <*dscp*>] [flow-label <*flowlabel*>] [time-range <*time-range-name*>]	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 <*fl*>] [time-range<time-range-name>]	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 {<*dPort*> | range <*dPortMin*> <*dPortMax*>}] [dscp <*dscp*>] [flow-label <*fl*>] [time-range<*time-range-name*>]	Creates an extended name-based UDP IPv6 access rule; the no form command deletes this name-based extended IPv6 access rule.
[no] {deny | permit} <*proto*> {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}}	Creates an extended name-based IPv6 access rule for other IPv6 protocols; the no form command deletes this name-based extended IPv6 access rule.

{<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [dscp <*dscp*>] [flow-label <*flowlabel*>] [time-range <*time-range-name*>]	
[no] {deny | permit} {<*sIPv6Prefix/sPrefixlen*> | any-source | {host-source <*sIPv6Addr*>}} {<*dIPv6Prefix/dPrefixlen*> | any-destination | {host-destination <*dIPv6Addr*>}} [dscp <*dscp*>] [flow-label <*flowlabel*>] [time-range <*time-range-name*>]	Creates an extended name-based IPv6 access rule; 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.

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 Port Mode/VLAN Interface Mode	
{ip|ipv6|mac|mac-ip} access-group <*acl-name*> {in|out} [traffic-statistic] **no {ip|ipv6|mac|mac-ip} access-group <*acl-name*> {in|out}**	Apply an access-list to the ingress or egress direction on the port; the no command deletes the access-list bound to the port.

5. Clear the filtering information of the specified port

Command	Explanation
Admin Mode	
clear access-group (in | out) statistic interface { <*interface-name*> | ethernet <*interface-name*> }	Clear the filtering information of the egress or ingress for the specified port.

1.3 ACL Example

Scenario 1:

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

Configuration description:

1. Create a proper ACL
2. Configuring packet filtering function
3. 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)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#ip access-group 110 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit

Configuration result:

Switch#show firewall
Firewall status: enable.
Firewall default rule: permit.
Switch#show access-lists
access-list 110(used 1 time(s)) 1 rule(s)
access-list 110 deny tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch#show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
the ingress acl use in firewall is 110, traffic-statistics Disable.

Scenario 2:

The configuration requirement is stated as below: The switch should drop all the 802.3 datagram with 00-12-11-23-xx-xx as the source MAC address coming from interface 10.

Configuration description:

1. Create the corresponding MAC ACL.
2. Configure datagram filtering.
3. Bind the ACL to the related interface.

The configuration steps are listed as below.

Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac untagged-802-3
Switch(config)#access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any tagged-802
Switch(config)#firewall enable
Switch(config)#interface ethernet1/0/10
Switch(Config-If-Ethernet1/0/10)#mac access-group 1100 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit

Configuration result:

Switch#show firewall
Firewall Status: Enable.

Switch #show access-lists
access-list 1100(used 1 time(s))
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac
untagged-802-3
access-list 1100 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac
Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
MAC Ingress access-list used is 1100,traffic-statistics Disable.

Scenario 3:

The configuration requirement is stated as below: The MAC address range of the network connected to the interface 10 of the switch is 00-12-11-23-xx-xx, and IP network is 10.0.0.0/24. FTP should be disabled and ping requests from outside network should be disabled.

Configuration description:

1. Create the corresponding access list.
2. Configure datagram filtering.
3. Bind the ACL to the related interface.

The configuration steps are listed as below.

Switch(config)#access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff any-destination-mac tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

Switch(config)#access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255

Switch(config)#firewall enable

Switch(config)#interface ethernet 1/0/10

Switch(Config-If-Ethernet1/0/10)#mac-ip access-group 3110 in

Switch(Config-Ethernet1/0/10)#exit

Switch(config)#exit

Configuration result:

Switch#show firewall

Firewall Status: Enable.

Switch#show access-lists

access-list 3110(used 1 time(s))

access-list 3110 deny 00-12-11-23-00-00 00-00-00-00-ff-ff

any-destination-mac

tcp 10.0.0.0 0.0.0.255 any-destination d-port 21

access-list 3110 deny any-source-mac 00-12-11-23-00-00 00-00-00-00-ff-ff icmp any-source 10.0.0.0 0.0.0.255

Switch #show access-group interface ethernet 1/0/10

interface name:Ethernet1/0/10

MAC-IP Ingress access-list used is 3110, traffic-statistics Disable.

Scenario 4:

The configuration requirement is stated as below: IPv6 protocol runs on the interface 600 of the switch. And the IPv6 network address is 2003:1:1:1::0/64. Users in the 2003:1:1:1:66::0/80 subnet should be disabled from accessing the outside network.

Configuration description:

1. Create the corresponding access list.
2. Configure datagram filting.
3. Bind the ACL to the related interface.

The configuration steps are listed as below.

Switch(config)#ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-destination
Switch(config)#ipv6 access-list 600 deny 2003:1:1:1::0/64 any-destination

Switch(config)#firewall enable
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#ipv6 access-group 600 in
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#exit

Configuration result:

Switch#show firewall
Firewall Status: Enable.

Switch#show ipv6 access-lists
Ipv6 access-list 600(used 1 time(s))
ipv6 access-list 600 deny 2003:1:1:1::0/64 any-source
ipv6 access-list 600 permit 2003:1:1:1:66::0/80 any-source

Switch #show access-group interface ethernet 1/0/10
interface name:Ethernet1/0/10
IPv6 Ingress access-list used is 600, traffic-statistics Disable.

Scenario 5:

The configuration requirement is stated as below: The interface 1, 2, 5, 7 belongs to vlan100, Hosts with 192.168.0.1 as its IP address should be disabled from accessing the listed interfaces.

Configuration description:

1. Create the corresponding access list.
2. Configure datagram filtering.

3. Bind the ACL to the related interface.

The configuration steps are listed as below.

Switch (config)#firewall enable

Switch (config)#vlan 100

Switch (Config-Vlan100)#switchport interface ethernet 1/0/1;2;5;7

Switch (Config-Vlan100)#exit

Switch (config)#access-list 1 deny host-source 192.168.0.1

Switch (config)#interface ethernet1/0/1;2;5;7

Switch (config-if-port-range)#ip access-group 1 in

Switch (Config-if-Vlan100)#exit

Configuration result:

Switch (config)#show access-group interface vlan 100

Interface VLAN 100:

Ethernet1/0/1: IP Ingress access-list used is 1, traffic-statistics Disable.

Ethernet1/0/2: IP Ingress access-list used is 1, traffic-statistics Disable.

Ethernet1/0/5: IP Ingress access-list used is 1, traffic-statistics Disable.

Ethernet1/0/7: IP Ingress access-list used is 1, traffic-statistics Disable.

1.4 ACL Troubleshooting

- Checking for entries in the ACL is done in a top-down order and ends whenever an entry is matched.
- Each ingress port can bind one MAC-IP ACL, one IP ACL, one MAC ACL, one IPv6 ACL (via the physical interface mode or Vlan interface mode).
- When binding four ACL and packet matching several ACL at the same time, the priority relations are as follows in a top-down order. If the priority is same, then the priority of configuration at first is higher.
  - Ingress IPv6 ACL
  - Ingress MAC-IP ACL
  - Ingress IP ACL
  - Ingress MAC 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.

Chapter 2 802.1x Configuration

2.1 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.

2.1.1 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.

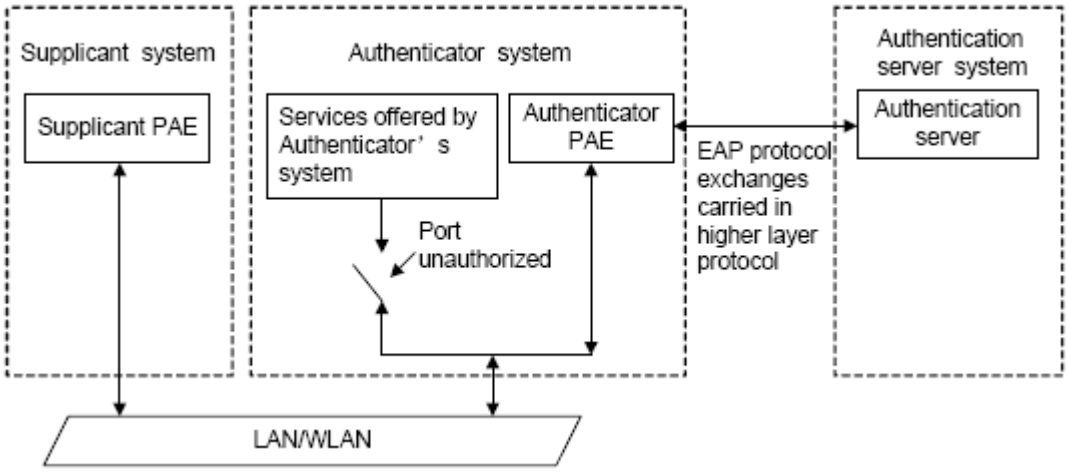


Fig 2-1 The Authentication Structure of 802.1x

- 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 start 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 does 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 unidirectional 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 unidirectional 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.

2.1.2 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.

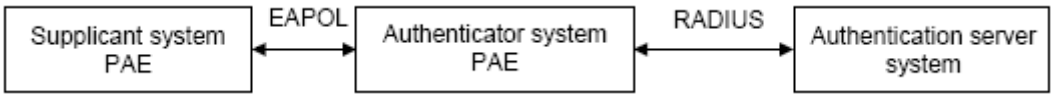


Fig 2-2 the Work Mechanism of 802.1x

- 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.

2.1.3 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.

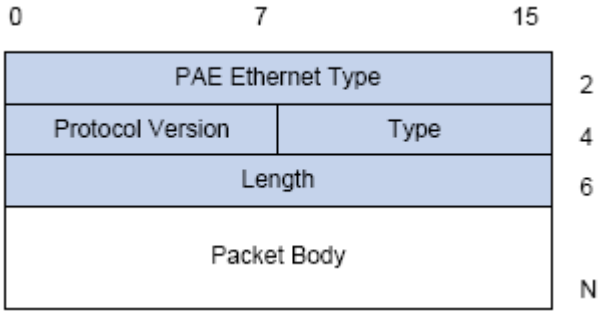


Fig 2-3 the Format of EAPOL Data Packet

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).

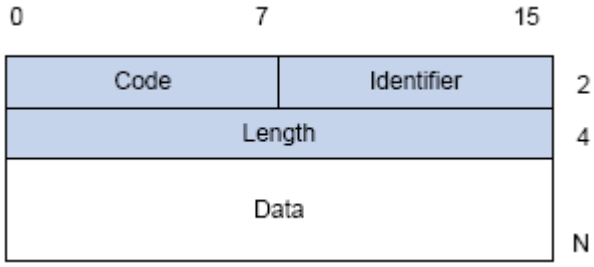


Fig 2-4 the Format of EAP Data Packets

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.

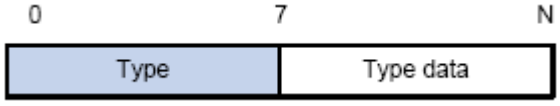


Fig 2-5 the Format of Data Domain in Request and Response Packets

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.

2.1.4 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.

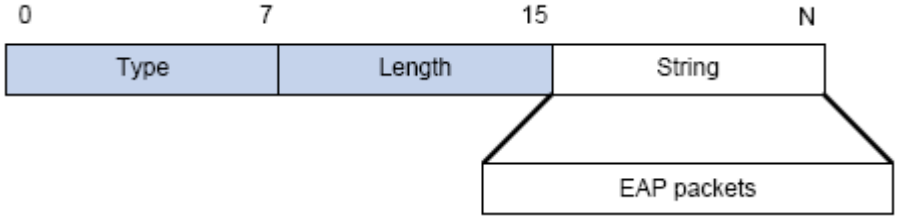


Fig 2-6 the Encapsulation of EAP-Message Attribute

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.

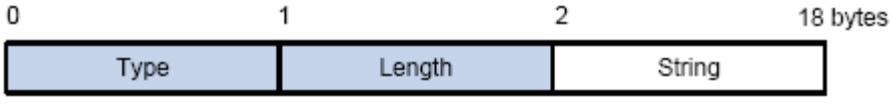


Fig 2-7 Message-Authenticator Attribute

2.1.5 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.

802.1 x systems 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.

2.1.5.1 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.

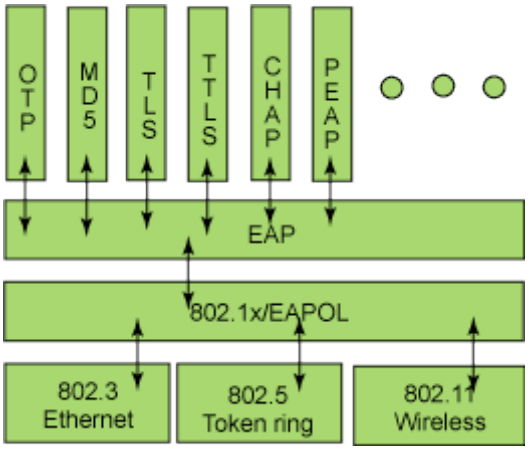


Fig 2-8 the Protocol Stack of EAP Authentication Method

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）

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.

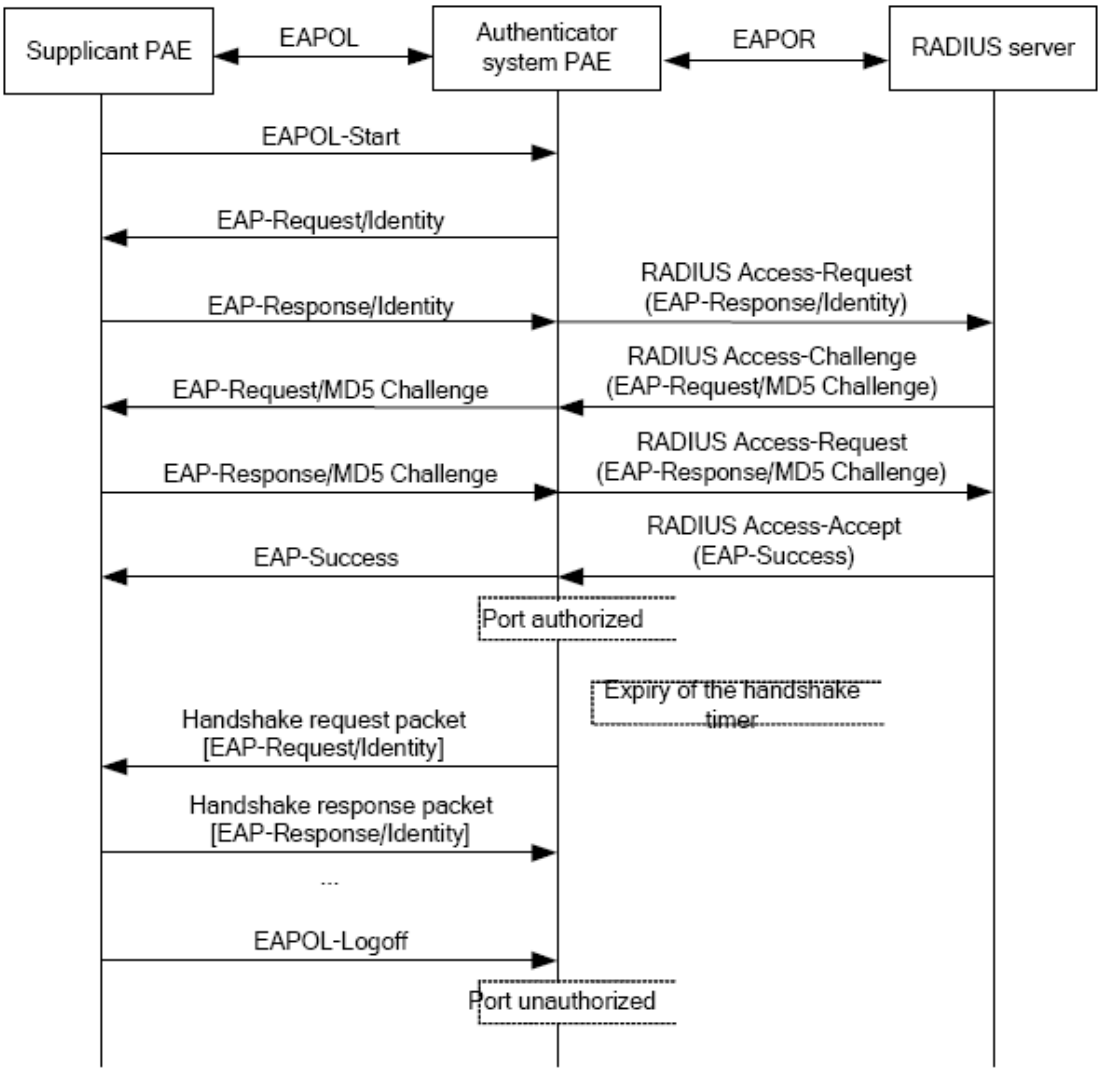


Fig 2-9 the Authentication Flow of 802.1x EAP-MD5

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.

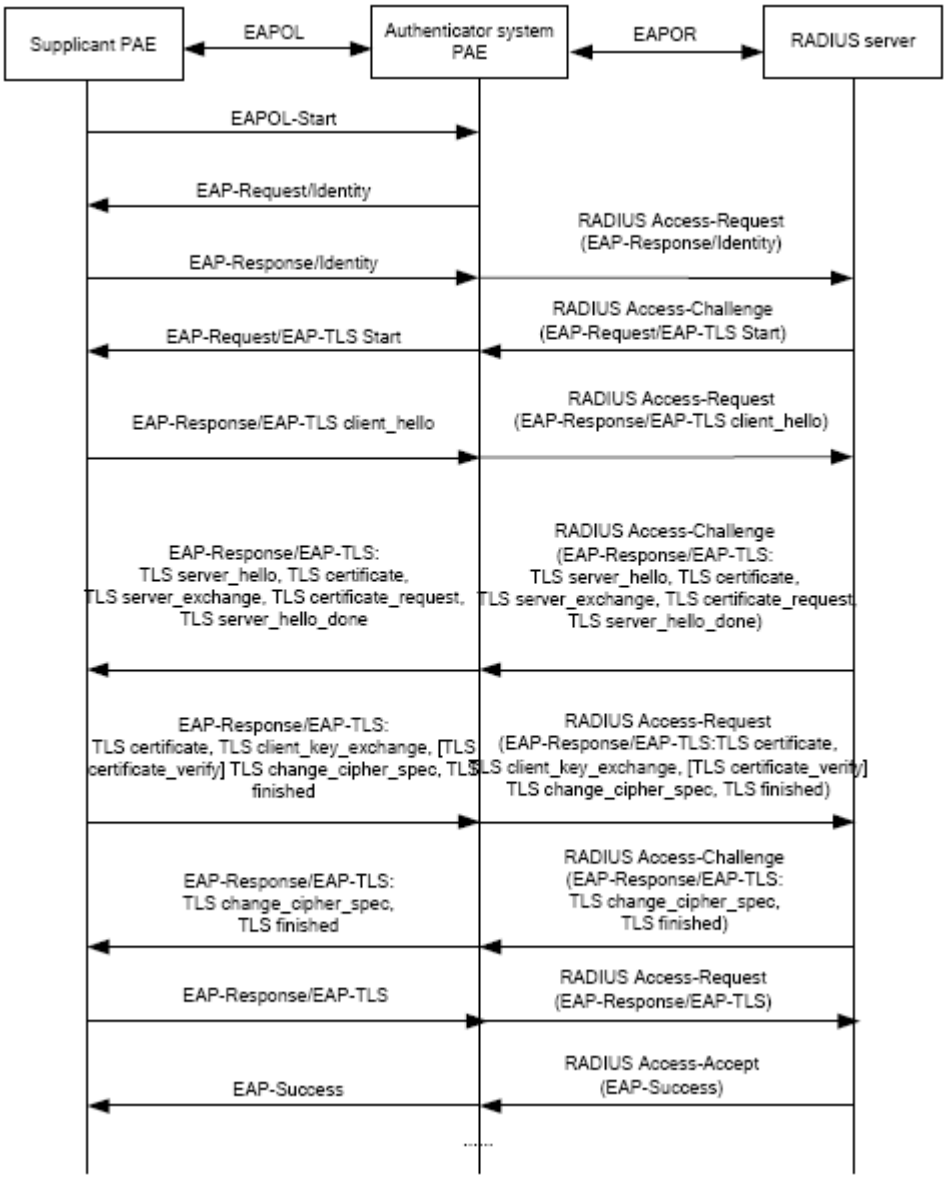


Fig 2-10 the Authentication Flow of 802.1x EAP-TLS

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.

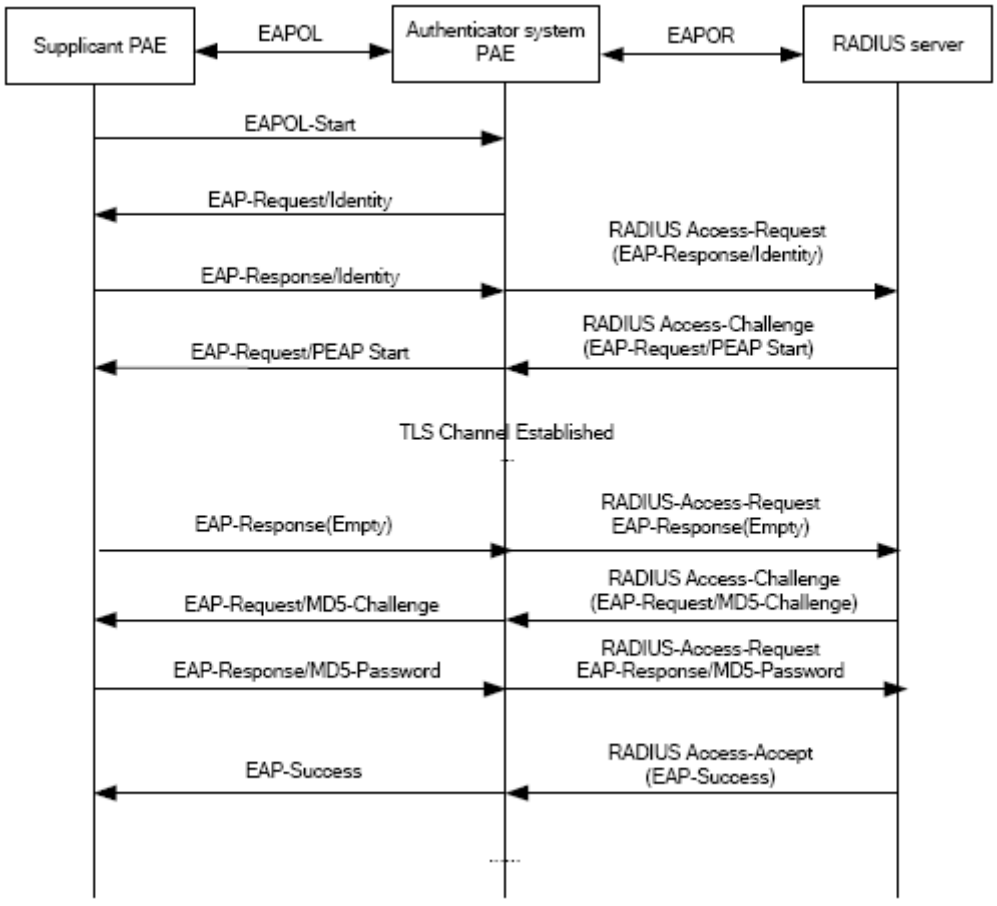


Fig 2-11 the Authentication Flow of 802.1x PEAP

2.1.5.2 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.

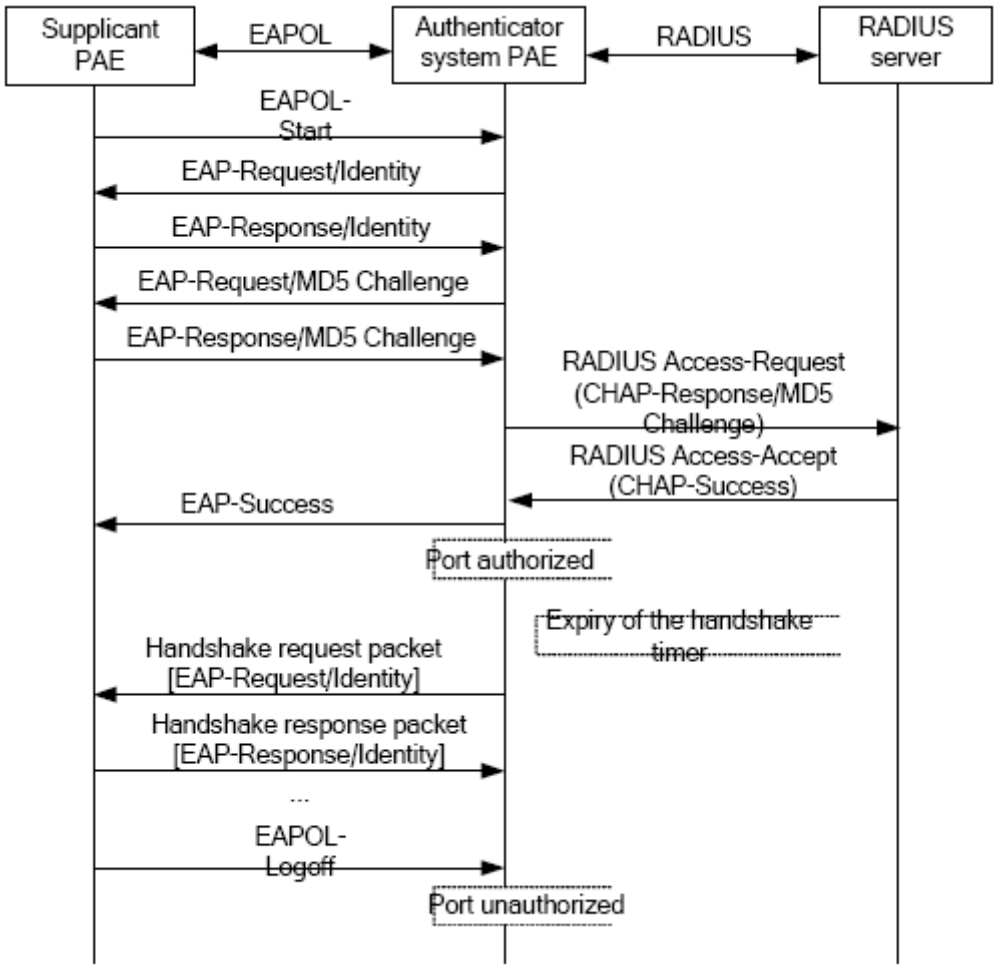


Fig 2-12 the Authentication Flow of 802.1x EAP Termination Mode

2.1.6 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.

For the maximum number of the authenticated users, the maximum number of IPv4 users supported by user-based is 400, the maximum number of IPv6 users supported by user-based is 800. mac-based relates to ratelimit value of switch, it can supports 4000 authenticated users, but it is recommended that the number of the authenticated users should not exceed 2000.

2.1.7 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.

2.2 802.1x Configuration Task List

802.1x Configuration Task List:

1. Enable IEEE 802.1x function
2. 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
3. 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 command disables the 802.1x function.
dot1x privateclient enable **no dot1x privateclient enable**	Enables the switch force client software using private 802.1x authentication packet format. The no command will disable this function.
dot1x user free-resource <*prefix*> <*mask*> **no dot1x user free-resource**	Sets free access network resource for unauthorized dot1x user. The no command close the resource.
dot1x unicast enable **no dot1x unicast enable**	Enable the 802.1x unicast passthrough function of switch; the no operation of this command will disable this function.

2. 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 command restores the default setting.

2) Configure port access management method

Command	Explanation
Port Mode	
dot1x port-method {macbased | portbased | userbased {standard | advanced}} **no dot1x port-method**	Sets the port access management method; the no 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 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 accessing the specified port, only used when the access control mode of the port is userbased; the no 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 command is used to delete the guest vlan.
dot1x portbased mode single-mode **no dot1x portbased mode single-mode**	Set the single-mode based on portbase authentication mode; the no command disables this function.

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 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 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 command sets EAP local end authentication.

3. 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 command restores the default setting.
dot1x re-authentication **no dot1x re-authentication**	Enables periodical supplicant authentication; the no 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 command restores the default value.
dot1x timeout re-authperiod <*seconds*> **no dot1x timeout re-authperiod**	Sets the supplicant re-authentication interval; the no 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 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.

2.3 802.1x Application Example

2.3.1 Examples of Guest Vlan Applications

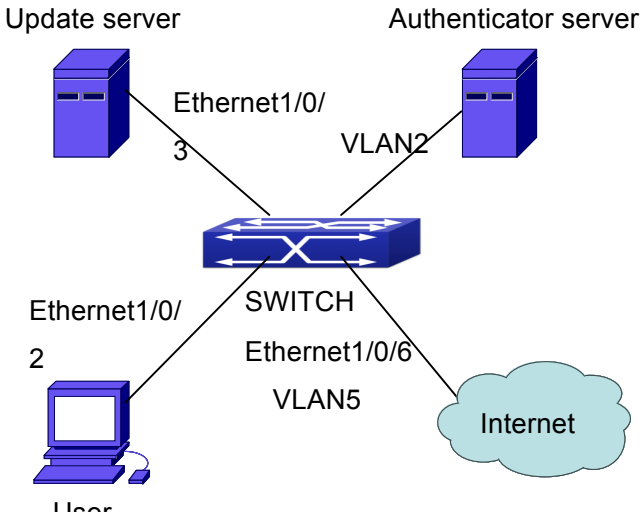


Fig 2-13 The Network Topology of Guest VLAN

Notes: in the figures in this session, E2 means Ethernet 1/0/2, E3 means Ethernet 1/0/3 and E6 means Ethernet 1/0/6.

As showed in the next figure, a switch accesses the network using 802.1x authentication, with a RADIUS server as its authentication server. Ethernet1/0/2, 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; Ethernet1/0/6, the port used by the switch to access the Internet is in VLAN5.

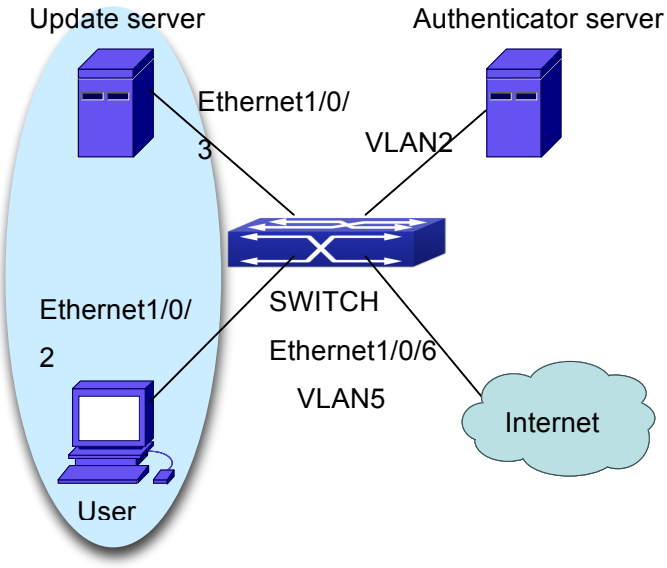


Fig 2-14 User Joining Guest VLAN

As illustrated in the up figure, on the switch port Ethernet1/0/2, 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 Ethernet1/0/2 is added into VLAN10, allowing the user to access the Update Server.

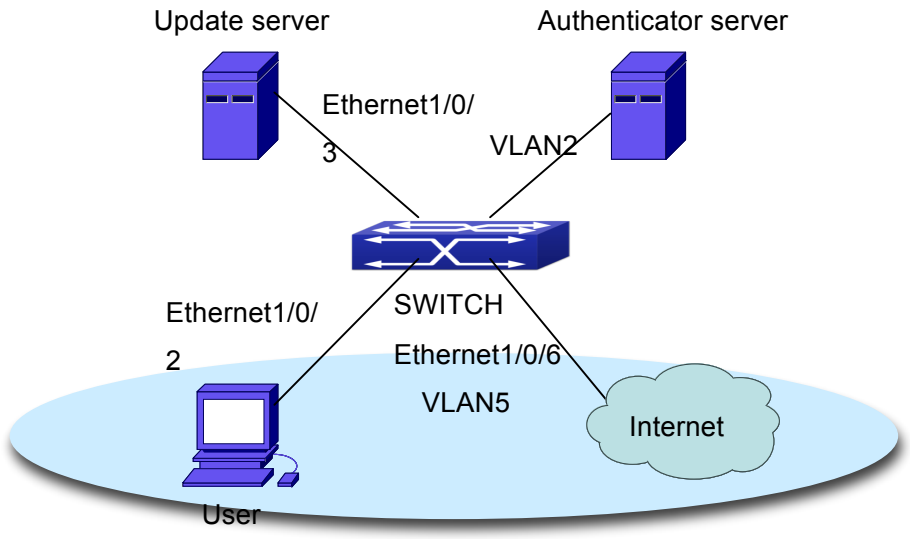


Fig 2-15 User Being Online, VLAN Being Offline

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 Ethernet1/0/6 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 Ethernet1/0/2

Switch(config)#interface ethernet1/0/2

Switch(Config-If-Ethernet1/0/2)#dot1x enable

Set the link type of the port as access mode.
Switch(Config-If-Ethernet1/0/2)#switch-port mode access

Set the access control mode on the port as portbased.
Switch(Config-If-Ethernet1/0/2)#dot1x port-method portbased

Set the access control mode on the port as auto.
Switch(Config-If-Ethernet1/0/2)#dot1x port-control auto

Set the port's Guest VLAN as 100.
Switch(Config-If-Ethernet1/0/2)#dot1x guest-vlan 100
Switch(Config-If-Ethernet1/0/2)#exit

Using the command of **show running-config** or **show interface ethernet1/0/2**, 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**.

2.3.2 Examples of IPv4 Radius Applications

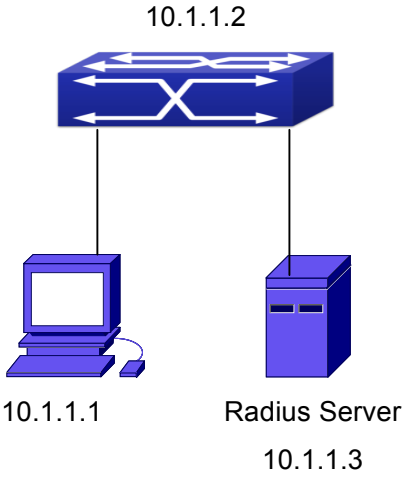


Fig 2-16 IEEE 802.1x Configuration Example Topology

The PC is connecting to port 1/0/2 of the switch; IEEE 802.1x authentication is enabled on port1/0/2; the access mode is the default MAC-based authentication. The switch IP address is 10.1.1.2. Any port other than port 1/0/2 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 1/0/2
Switch(Config-Ethernet1/0/2)#dot1x enable
Switch(Config-Ethernet1/0/2)#dot1x port-control auto
Switch(Config-Ethernet1/0/2)#exit
```

2.3.3 Examples of IPv6 Radius Application

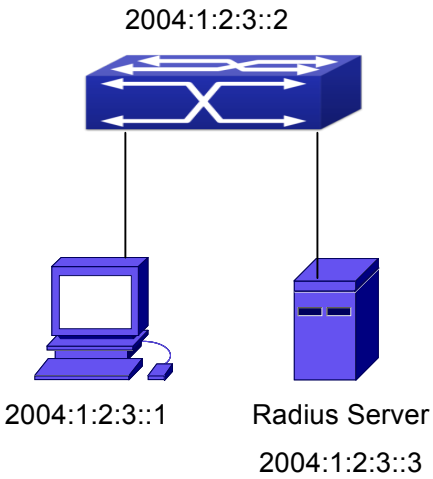


Fig 2-17 IPv6 Radius

Connect the computer to the interface 1/0/2 of the switch, and enable IEEE802.1x on interface1/0/2. Use MAC based authentication. Configure the IP address of the switch as 2004:1:2:3::2, and connect the switch with any interface except interface 1/0/2 to the RADIUS authentication server. Configure the IP address of the RADIUS server to be 2004:1:2:3::3. Use the default ports 1812 and 1813 for authentication and accounting

respectively. Install the IEEE802.1x authentication client software on the computer, and use the client for IEEE802.1x authentication.

The detailed configurations are listed as below:

```
Switch(config)#interface vlan 1
Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64
Switch(Config-if-vlan1)#exit
Switch(config)#radius-server authentication host 2004:1:2:3::3
Switch(config)#radius-server accounting host 2004:1:2:3::3
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
Switch(config)#dot1x enable
Switch(config)#interface ethernet 1/0/2
Switch(Config-If-Ethernet1/0/2)#dot1x enable
Switch(Config-If-Ethernet1/0/2)#dot1x port-control auto
Switch(Config-If-Ethernet1/0/2)#exit
```

2.4 802.1x Troubleshooting

It is possible that 802.1x be configured on ports and 802.1x authentication be set to auto, t switch can'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 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.

Chapter 3 The Number Limitation Function of MAC and IP in Port, VLAN Configuration

3.1 Introduction to the Number Limitation Function of MAC and IP in Port, VLAN

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 MAC and IP in port, VLAN. 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 MAC, ARP and ND 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.

3.2 The Number Limitation Function of MAC and IP in Port, VLAN Configuration Task Sequence

1. Enable the number limitation function of MAC and IP on ports
2. Enable the number limitation function of MAC and IP in VLAN
3. Configure the timeout value of querying dynamic MAC
4. Configure the violation mode of ports
5. Display and debug the relative information of number limitation of MAC and IP on ports

1. Enable the number limitation function of MAC and 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 dynamic maximum**	Enable and disable the number limitation function of ND on the ports.

2. Enable the number limitation function of MAC and IP in VLAN

Command	Explanation
VLAN configuration mode	
vlan mac-address dynamic maximum <*value*> **no vlan mac-address dynamic maximum**	Enable and disable the number limitation function of MAC in the VLAN.
Interface configuration mode	
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. Configure the violation mode of ports

Command	Explanation
Port mode	

switchport mac-address violation {protect | shutdown} [recovery <*5-3600*>] **no switchport mac-address violation**	Set the violation mode of the port, the no command restores the violation mode to **protect**.

5. Display and debug the relative information of number limitation of MAC and 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 ip arp count**	All kinds of debug information when limiting the number of ARP in VLAN.
debug ipv6 nd count **no debug ipv6 nd count**	All kinds of debug information when limiting the number of MAC in VLAN.

3.3 The Number Limitation Function of MAC and IP in Port, VLAN Typical Examples

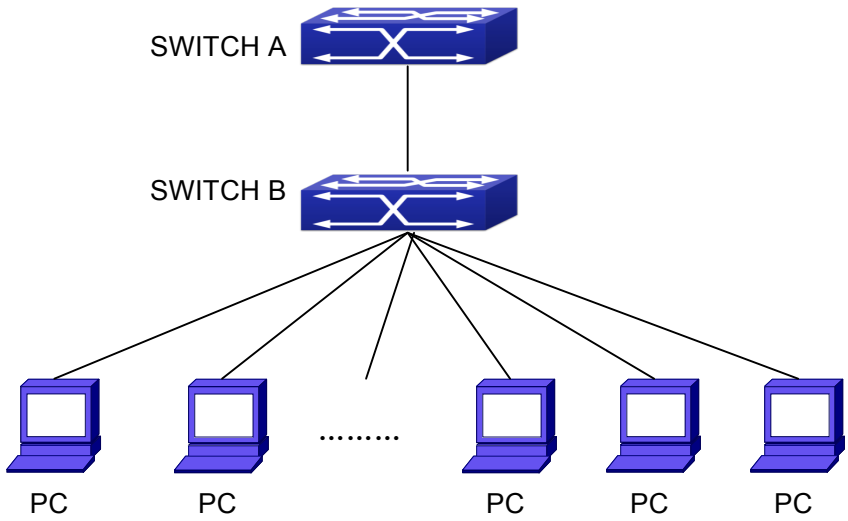


Fig 3-1 The Number Limitation of MAC and IP in Port, VLAN Typical Configuration Example

In the network topology above, SWITCH B connects to many PC users, before enabling the number limitation function of MAC and IP in Port, VLAN, 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, ARP cheating, it will be easy for them to fill the MAC, ARP list entries of the switch, causing successful DOS attacks. Limiting the MAC, ARP, ND list entry can prevent DOS attack.

On port 1/0/1 of SWITCH A, set the max number can be learnt of dynamic MAC address as 20, 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)#interface ethernet 1/0/1
Switch (Config-If-Ethernet1/0/1)#switchport mac-address dynamic maximum 20
Switch (Config-If-Ethernet1/0/1)#switchport arp dynamic maximum 20
Switch (Config-If-Ethernet1/0/1)#switchport nd dynamic maximum 10
Switch (Config-if-Vlan1)#vlan mac-address dynamic maximum 30

3.4 The Number Limitation Function of MAC and IP in Port, VLAN Troubleshooting Help

The number limitation function of MAC and IP in Port, VLAN 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 MAC and IP in Port, VLAN, 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 4 Operational Configuration of AM Function

4.1 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.

4.2 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
Port Mode	
am port **no am port**	Enable/disable AM function on the port. When the AM function is enabled on the port, no IP or ARP message will be forwarded by default.

3. Configure the forwarding IP

Command	Explanation
Port Mode	
am ip-pool <*ip-address*> <*num*> **no am ip-pool <*ip-address*> <*num*>**	Configure the forwarding IP of the port.

4. Configure the forwarding MAC-IP

Command	Explanation
Port 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 port.

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
Global Configuration Mode	
show am [interface <*interface-name*>]	Display the AM configuration information of one port or all ports.

4.3 AM Function Example

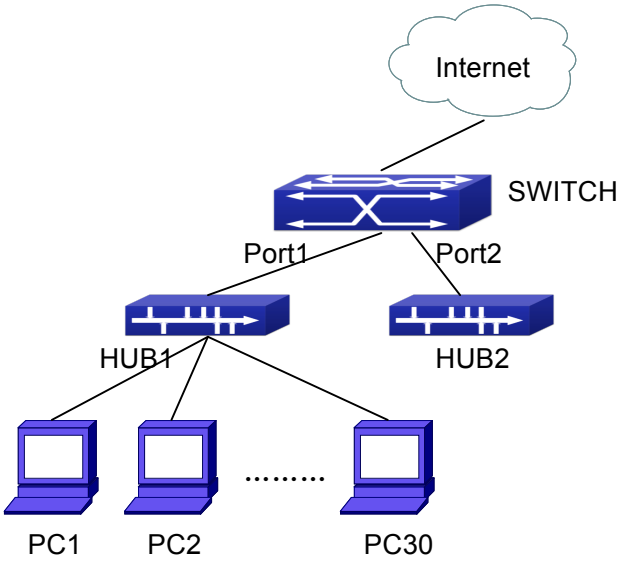


Fig 4-1 a typical configuration example of AM function

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 ethernet1/0/1
Switch(Config-If-Ethernet 1/0/1)#am port
Switch(Config-If-Ethernet 1/0/1)#am ip-pool 10.10.10.1 10

4.4 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 5 TACACS+ Configuration

5.1 Introduction to TACACS+

TACACS+ terminal access controller access control protocol is a protocol similar to the radius protocol for control the terminal access to the network. Three independent functions of Authentication, Authorization, Accounting are also available in this protocol. Compared with RADIUS, the transmission layer of TACACS+ protocol is adopted with TCP protocol, further with the packet head (except for standard packet head) encryption, this protocol is of a more reliable transmission and encryption characteristics, and is more adapted to security control.

According to the characteristics of the TACACS+ (Version 1.78), we provide TACACS+ authentication function on the switch, when the user logs, such as telnet, the authentication of user name and password can be carried out with TACACS+.

5.2 TACACS+ Configuration Task List

1. Configure the TACACS+ authentication key
2. Configure the TACACS+ server
3. Configure the TACACS+ authentication timeout time
4. Configure the IP address of the RADIUS NAS

1. Configure the TACACS+ authentication key

Command	Explanation
Global Mode	
tacacs-server key {0 | 7}<*string*> **no tacacs-server key**	Configure the TACACS+ server key; the "**no tacacs-server key**" command deletes the key.

2. Configure TACACS+ server

Command	Explanation
Global Mode	

tacacs-server authentication host <*ip-address*> [port <*port-number*>] [timeout <*seconds*>] [key {0 | 7} <*string*>] [primary] **no tacacs-server authentication host <*ip-address*>**	Configure the IP address, listening port number, the value of timeout timer and the key string of the TACACS+ server; the no form of this command deletes the TACACS+ authentication server.

3. Configure the TACACS+ authentication timeout time

Command	Explanation
Global Mode	
tacacs-server timeout <*seconds*> **no tacacs-server timeout**	Configure the authentication timeout for the TACACS+ server, the "**no tacacs-server timeout**" command restores the default configuration.

4. Configure the IP address of the TACACS+ NAS

Command	Explanation
Global Mode	
tacacs-server nas-ipv4 <*ip-address*> **no tacacs-server nas-ipv4**	To configure the source IP address for the TACACS+ packets for the switch.

5.3 TACACS+ Scenarios Typical Examples

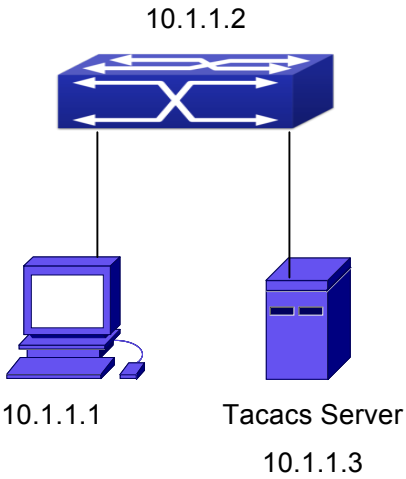


Fig 5-1 TACACS Configuration

A computer connects to a switch, of which the IP address is 10.1.1.2 and connected with a TACACS+ authentication server; IP address of the server is 10.1.1.3 and the authentication port is defaulted at 49, set telnet log on authentication of the switch as tacacs local, via using TACACS+ authentication server to achieve telnet user

authentication.

```
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)#tacacs-server authentication host 10.1.1.3
Switch(config)#tacacs-server key test
Switch(config)#authentication line vty login tacacs
```

5.4 TACACS+ Troubleshooting

In configuring and using TACACS+, the TACACS+ may fail to authentication due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- First good condition of the TACACS+ server physical connection.
- Second all interface and link protocols are in the UP state (use "**show interface**" command).
- Then ensure the TACACS+ key configured on the switch is in accordance with the one configured on TACACS+ server.
- Finally ensure to connect to the correct TACACS+ server.

Chapter 6 RADIUS Configuration

6.1 Introduction to RADIUS

6.1.1 AAA and RADIUS Introduction

AAA is short for Authentication, Authorization and Accounting, it provide a consistency framework for the network management safely. According to the three functions of Authentication, Authorization, Accounting, the framework can meet the access control for the security network: which one can visit the network device, which access-level the user can have and the accounting for the network resource.

RADIUS (Remote Authentication Dial in User Service), is a kind of distributed and client/server protocol for information exchange. The RADIUS client is usually used on network appliance to implement AAA in cooperation with 802.1x protocol. The RADIUS server maintains the database for AAA, and communicates with the RADIUS client through RADIUS protocol. The RADIUS protocol is the most common used protocol in the AAA framework.

6.1.2 Message structure for RADIUS

The RADIUS protocol uses UDP to deliver protocol packets. The packet format is shown as below.

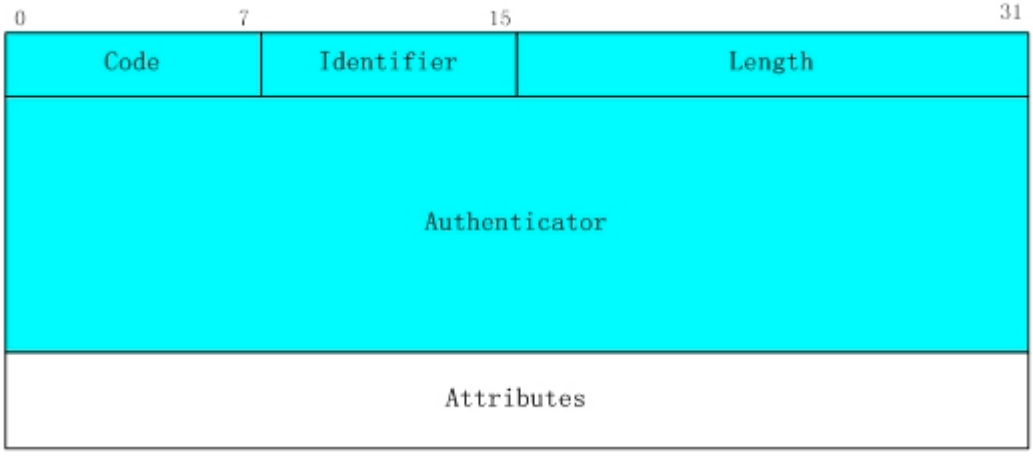


Fig 6-1 Message structure for RADIUS

Code field(1octets): is the type of the RADIUS packet. Available value for the Code field is

show as below:

1 Access-Request
2 Access-Accept
3 Access-Reject
4 Accounting-Request
5 Accounting-Response
11 Access-Challenge

Identifier field (1 octet): Identifier for the request and answer packets.

Length field (2 octets): The length of the overall RADIUS packet, including Code, Identifier, Length, Authenticator and Attributes

Authenticator field (16 octets): used for validation of the packets received from the RADIUS server. Or it can be used to carry encrypted passwords. This field falls into two kinds: the Request Authenticator and the Response Authenticator.

Attribute field: used to carry detailed information about AAA. An Attribute value is formed by Type, Length, and Value fields.

☞ Type field (1 octet), the type of the attribute value, which is shown as below:

Property	Type of property	Property	Type of property
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-Id	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network

17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-Id	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

- Length field (1 octet), the length in octets of the attribute including Type, Length and Value fields.
- Value field, value of the attribute whose content and format is determined by the type and length of the attribute.

6.2 RADIUS Configuration Task List

1. Enable the authentication and accounting function
2. Configure the RADIUS authentication key
3. Configure the RADIUS server
4. Configure the parameter of the RADIUS service
5. Configure the IP address of the RADIUS NAS

1. Enable the authentication and accounting function

Command	Explanation
Global Mode	
aaa enable **no aaa enable**	To enable the AAA authentication function. The no form of this command will disable the AAA authentication function.
aaa-accounting enable **no aaa-accounting enable**	To enable AAA accounting. The no form of this command will disable AAA accounting.
aaa-accounting update {enable|disable}	Enable or disable the update accounting function.

2. Configure the RADIUS authentication key

Command	Explanation
Global Mode	

radius-server key {0 | 7} <*string*> **no radius-server key**	To configure the encryption key for the RADIUS server. The no form of this command will remove the configured key.

3. Configure the RADIUS server

Command	Explanation
Global Mode	
radius-server authentication host {<*ipv4-address*> | <*ipv6-address*>} [port <*port-number*>] [key *{0 | 7}* <*string*>] [primary] [access-mode {dot1x | telnet}] **no radius-server authentication host {<*ipv4-address*> | <*ipv6-address*>**	Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server; the no command deletes the RADIUS accounting server.
radius-server accounting host {<*ipv4-address*> | <*ipv6-address*>} [port <*port-number*>] [key {*0* | 7} <*string*>] [primary] **no radius-server accounting host {<*ipv4-address*> | <*ipv6-address*>}**	Specifies the IPv4/IPv6 address and the port number, whether be primary server for RADIUS accounting server; the no command deletes the RADIUS accounting server.

4. Configure the parameter of the RADIUS service

Command	Explanation
Global Mode	
radius-server dead-time <*minutes*> **no radius-server dead-time**	To configure the interval that the RADIUS becomes available after it is down. The no form of this command will restore the default configuration.
radius-server retransmit <*retries*> **no radius-server retransmit**	To configure retry times for the RADIUS packets. The no form of this command restores the default configuration.
radius-server timeout <*seconds*> **no radius-server timeout**	To configure the timeout value for the RADIUS server. The no form of this command will restore the default configuration.

radius-server accounting-interim-update timeout *<seconds>* **no radius-server accounting-interim-update timeout**	To configure the update interval for accounting. The no form of this command will restore the default configuration.

5. Configure the IP address of the RADIUS NAS

Command	Explanation
Global Mode	
radius nas-ipv4 *<ip-address>* **no radius nas-ipv4**	To configure the source IP address for the RADIUS packets for the switch.
radius nas-ipv6 *<ipv6-address>* **no radius nas-ipv6**	To configure the source IPv6 address for the RADIUS packets for the switch.

6.3 RADIUS Typical Examples

6.3.1 IPv4 Radius Example

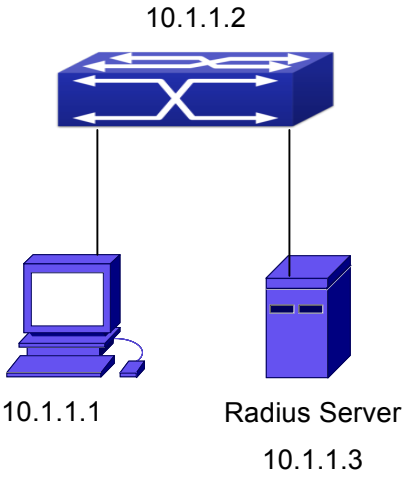


Fig 6-2 The Topology of IEEE802.1x configuration

A computer connects to a switch, of which the IP address is 10.1.1.2 and connected with a RADIUS authentication server without Ethernet1/0/2; IP address of the server is 10.1.1.3 and the authentication port is defaulted at 1812, accounting port is defaulted at 1813.

Configure steps as 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

6.3.2 IPv6 RadiusExample

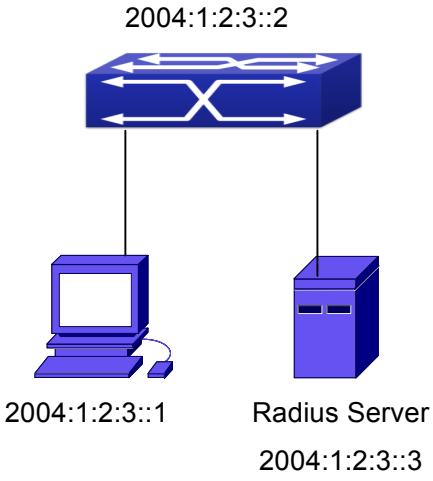


Fig 6-3 The Topology of IPv6 Radius configuration

A computer connects to a switch, of which the IP address is 2004:1:2:3::2 and connected with a RADIUS authentication server without Ethernet1/0/2; IP address of the server is 2004:1:2:3::3 and the authentication port is defaulted at 1812, accounting port is defaulted at 1813.

Configure steps as below:

Switch(config)#interface vlan 1

Switch(Config-if-vlan1)#ipv6 address 2004:1:2:3::2/64

Switch(Config-if-vlan1)#exit

Switch(config)#radius-server authentication host 2004:1:2:3::3

Switch(config)#radius-server accounting host 2004:1:2:3::3

Switch(config)#radius-server key test

Switch(config)#aaa enable

Switch(config)#aaa-accounting enable

6.4 RADIUS Troubleshooting

In configuring and using RADIUS, the RADIUS may fail to authentication due to reasons such as physical connection failure or wrong configurations. The user should ensure the following:

- ☞ First make sure good condition of the RADIUS server physical connection
- ☞ Second all interface and link protocols are in the UP state (use "**show interface**" command)
- ☞ Then ensure the RADIUS key configured on the switch is in accordance with the one configured on RADIUS server
- ☞ Finally ensure to connect to the correct RADIUS server

If the RADIUS authentication problem remains unsolved, please use **debug aaa** and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to the technical server center of our company.

Chapter 7 SSL Configuration

7.1 Introduction to SSL

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 barriers 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 Network. The SSL protocol uses the public-key encryption, and has become the industry standard for secure communication on internet for Web browsing. The Web browser integrates HTTP and SSL to realize secure communication.

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 is provided by SSL protocols have below three characteristics:

- ☞ 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).

7.1.1 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

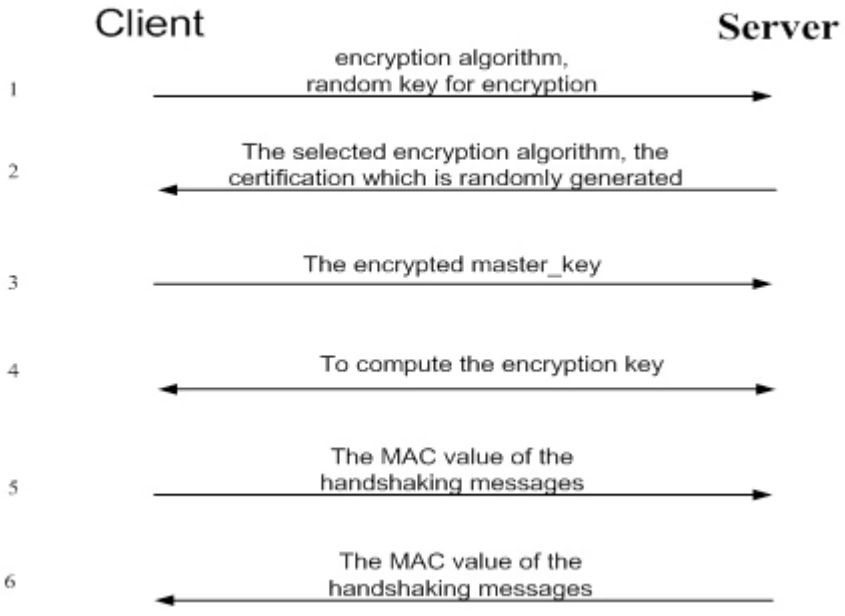
TCP. If the mechanism of the data forwarding in the lower layer is reliable, the data read-in the network will be forwarded to the other program in sequence, lose packet and re-forwarding will not appear. A lot of transmission protocols can provide such kind of service in theory, but in actual application, 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.

SSL 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 authentic, but the private certification keys generated by SSL 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:



7.2 SSL Configuration Task List

1. Enable/disable SSL function
2. Configure/delete port number by SSL used
3. Configure/delete secure cipher suite by SSL used
4. Maintenance and diagnose for the SSL function

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 port number by SSL used, the"**no ip http secure-port**" command deletes the port 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.

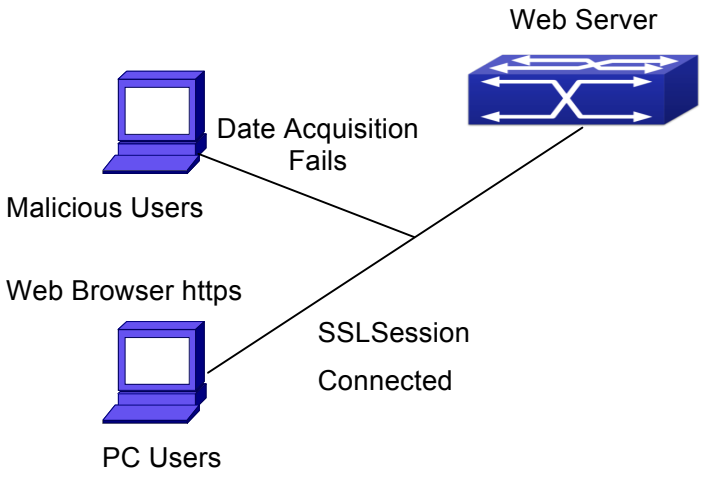
4. Maintenance and diagnose for the SSL function

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.

7.3 SSL Typical Example

When the Web function is enabled on the switch, SSL 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.

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.



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

7.4 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 the default port number if configured port number, pay attention to the port number when input the web wide;
- If SSL is enabled, SSL should be restarted after changes on the port configuration and encryption configuration;
- IE 7.0 or above should be used for use of des-cbc-sha;
- If the SSL problems remain unsolved after above try, please use debug SSL and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to technical server center of our company.

Chapter 8 IPv6 Security RA Configuration

8.1 Introduction to IPv6 Security RA

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.

8.2 IPv6 Security RA Configuration Task Sequence

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 distrust port and whether globally security RA is enabled.

8.3 IPv6 Security RA Typical Examples

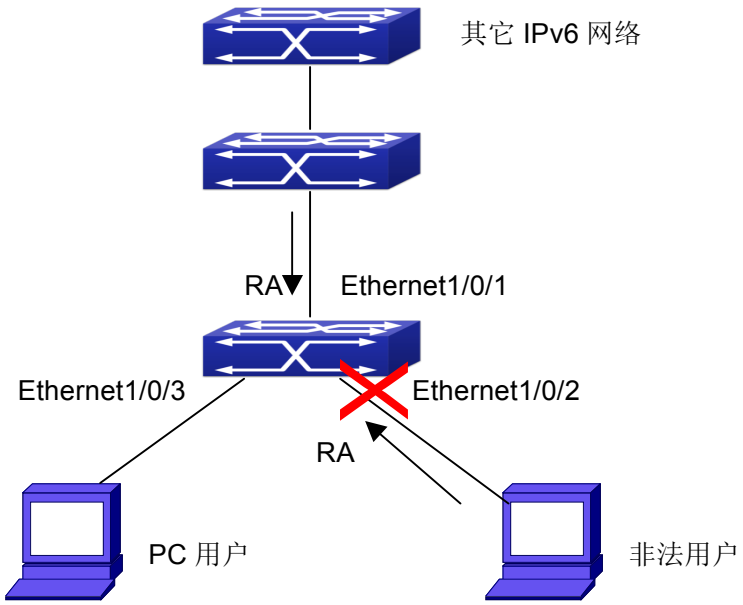


Fig 8-1 IPv6 Security RA sketch map

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 1/0/2 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-Ethernet1/0/2)# ipv6 security-ra enable

8.4 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.

Chapter 9 VLAN-ACL Configuration

9.1 Introduction to VLAN-ACL

The user can configure ACL policy to VLAN to implement the accessing control of all ports in VLAN, and VLAN-ACL enables the user to expediently manage the network. The user only needs to configure ACL policy in VLAN, the corresponding ACL action can takes effect on all member ports of VLAN, but it does not need to solely configure on each member port.

When VLAN ACL and Port ACL are configured at the same time, the principle of denying firstly is used. When the packets match VLAN ACL and Port ACL at the same time, as long as one rule is drop, then the final action is drop.

Egress ACL can implement the filtering of the packets on egress and ingress direction, the packets match the specific rules can be allowed or denied. ACL can support IP ACL, MAC ACL, MAC-IP ACL, IPv6 ACL. Ingress direction of VLAN can bind four kinds of ACL at the same time, there are four resources on egress direction of VLAN, IP ACL and MAC ACL engage one resource severally, MAC-IP ACL and IPv6 ACL engage two resources severally, so egress direction of VLAN can not bind four kinds of ACL at the same time. When binding three kinds of ACL at the same time, it should be the types of IP, MAC, MAC-IP or IP, MAC, IPv6. When binding two kinds of ACL at the same time, any combination of ACL type is valid. Each type can only apply one on a VLAN.

9.2 VLAN-ACL Configuration Task List

1. Configure VLAN-ACL of IP type
2. Configure VLAN-ACL of MAC type
3. Configure VLAN-ACL of MAC-IP
4. Configure VLAN-ACL of IPv6 type
5. Show configuration and statistic information of VLAN-ACL
6. Clear statistic information of VLAN-ACL

1. Configure VLAN-ACL of IP type

Command	Explanation
Global mode	

vacl ip access-group {*<1-299>* | WORD} {in | out} [traffic-statistic] vlan WORD **no vacl ip access-group {*<1-299>* | WORD} {in | out} vlan WORD**	Configure or delete IP VLAN-ACL.

2. Configure VLAN-ACL of MAC type

Command	Explanation
Global mode	
vacl mac access-group {*<700-1199>* | WORD} {in | out} [traffic-statistic] vlan WORD **no vacl mac access-group {*<700-1199>* | WORD} {in | out} vlan WORD**	Configure or delete MAC VLAN-ACL.

3. Configure VLAN-ACL of MAC-IP

Command	Explanation
Global mode	
vacl mac-ip access-group {*<3100-3299>* | WORD} {in | out} [traffic-statistic] vlan WORD **no vacl mac-ip access-group {*<3100-3299>* | WORD} {in | out} vlan WORD**	Configure or delete MAC-IP VLAN-ACL.

4. Configure VLAN-ACL of IPv6 type

Command	Explanation
Global mode	
vacl ipv6 access-group (*<500-699>* | WORD) {in | out} (traffic-statistic|) vlan WORD **no ipv6 access-group {*<500-699>* | WORD} {in | out} vlan WORD**	Configure or delete IPv6 VLAN-ACL.

5. Show configuration and statistic information of VLAN-ACL

Command	Explanation
Admin mode	
show vacl [in | out] vlan [*<vlan-id>*]	Show the configuration and the statistic information of VACL.

6. Clear statistic information of VLAN-ACL

Command	Explanation
Admin mode	
clear vacl [in | out] statistic vlan [<*vlan-id*>]	Clear the statistic information of VACL.

9.3 VLAN-ACL Configuration Example

A company's network configuration is as follows, all departments are divided by different VLANs, technique department is Vlan1, finance department is Vlan2. It is required that technique department can access the outside network at timeout, but finance department are not allowed to access the outside network at any time for the security. Then the following policies are configured:

- Set the policy VACL_A for technique department. At timeout they can access the outside network, the rule as permit, but other times the rule as deny, and the policy is applied to Vlan1.
- Set the policy VACL_B of ACL for finance department. At any time they can not access the outside network, but can access the inside network with no limitation, and apply the policy to Vlan2.

Network environment is shown as below:

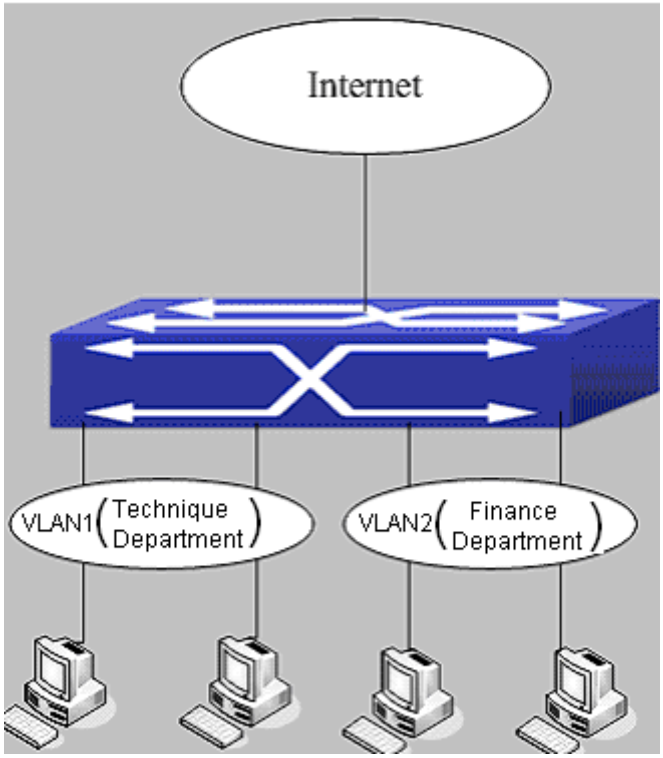


Fig 9-1 VLAN-ACL configuration example

Configuration example:

1) First, configure a timerange, the valid time is the working hours of working day:

Switch(config)#time-range t1

Switch(config-time-range-t1)#periodic weekdays 9:00:00 to 12:00:00

Switch(config-time-range-t1)#periodic weekdays 13:00:00 to 18:00:00

2) Configure the extended acl_a of IP, at working hours it only allows to access the resource within the internal network (such as 192.168.0.255).

Switch(config)# ip access-list extended vacl_a

Switch(config-ip-ext-nacl-vacl_a)# permit ip any-source 192.168.0.0 0.0.0.255 time-range t1

Switch(config-ip-ext-nacl-vacl_a)# deny ip any-source any-destination time-range t1

3) Configure the extended acl_b of IP, at any time it only allows to access resource within the internal network (such as 192.168.1.255).

Switch(config)#ip access-list extended vacl_b

Switch(config-ip-ext-nacl-vacl_a)# permit ip any-source 192.168.1.0 0.0.0.255

Switch(config-ip-ext-nacl-vacl_a)# deny ip any-source any-destination

4) Apply the configuration to VLAN

Switch(config)#vacl ip access-group vacl_a in vlan 1

Switch(config)#vacl ip access-group vacl_b in vlan 2

9.4 VLAN-ACL Troubleshooting

- ☞ When VLAN ACL and Port ACL are configured at the same time, the principle of denying firstly is used. When the packets match VLAN ACL and Port ACL at the same time, as long as one rule is drop, then the final action is drop.
- ☞ Each ACL of different types can only apply one on a VLAN, such as the basic IP ACL, each VLAN can applies one only.

Chapter 10 MAB Configuration

10.1 Introduction to MAB

In actual network existing the device which can not install the authentication client, such as printer, PDA devices, they can not process 802.1x authentication. However, to access the network resources, they need to use MAB authentication to replace 802.1x authentication.

MAB authentication is a network accessing authentication method based on the accessing port and the MAC address of MAB user. The user needn't install any authentication client, after the authentication device receives ARP packets sent by MAB user, it will authenticate the MAC address of the MAB user and there is the corresponding authentication information in the authentication server, the matched packets of the port and the source MAC are allowed to pass when the authentication is successful. MAB user didn't need to input the username and password manually in the process of authentication.

At present, MAB authentication device only supports RADIUS authentication method. There is the selection method for the authentication username and password: use the MAC address of the MAB user as the username and password, or the fixed username and password (all users use the configured username and password to authenticate).

10.2 MAB Configuration Task List

MAB Configuration Task List:

1. Enable MAB function
   1) Enable global MAB function
   2) Enable port MAB function
2. Configure MAB authentication username and password
3. Configure MAB parameters
   1) Configure guest-vlan
   2) Configure the binding-limit of the port
   3) Configure the reauthentication time
   4) Configure the offline detection time
   5) Configure other parameters

1. Enable MAB function

Command	Explanation
Global Mode	
mac-authentication-bypass enable **no mac-authentication-bypass enable**	Enable the global MAB authentication function.
Port Mode	
mac-authentication-bypass enable **no mac-authentication-bypass enable**	Enable the port MAB authentication function.

2. Configure MAB authentication username and password

Command	Explanation
Global Mode	
mac-authentication-bypass username-format {mac-address | {fixed username WORD password WORD}}	Set the authentication mode of MAB authentication function.

3. Configure MAB parameters

Command	Explanation
Port Mode	
mac-authentication-bypass guest-vlan *<1-4094>* **no mac-authentication-bypass guest-vlan**	Set guset vlan of MAB authentication, only Hybrid port uses this command, it is not take effect on access port.
mac-authentication-bypass binding-limit *<1-100>* **no mac-authentication-bypass binding-limit**	Set the max MAB binding-limit of the port.
Global Mode	
mac-authentication-bypass timeout reauth-period *<1-3600>* **no mac-authentication-bypass timeout reauth-period**	Set the reauthentication interval after the authentication is unsuccessful.

mac-authentication-bypass timeout offline-detect （**0**｜**<*60-7200*>**） **no** mac-authentication-bypass timeout offline-detect	Set offline detection interval.
mac-authentication-bypass timeout quiet-period <*1-60*> **no mac-authentication-bypass timeout quiet-period**	Set quiet-period of MAB authentication.
mac-authentication-bypass timeout stale-period <*0-60*> no mac-authentication-bypass timeout stale-period	Set the time that delete the binding after the port is down.
mac-authentication-bypass timeout linkup-period <*0-30*> **no mac-authentication-bypass timeout linkup-period**	To obtain IP again, set the interval of down/up when MAB binding is changing into VLAN.
mac-authentication-bypass spoofing-garp-check enable **no mac-authentication-bypass spoofing-garp-check enable**	Enable the spoofing-garp-check function, MAB function will not deal with spoofing-garp any more; the no command disables the function.
authentication mab {radius | none} **no authentication mab**	Configure the authentication mode and priority of MAC address, the no command restores the default authentication mode.

10.3 MAB Example

Example:

The typical example of MAB authentication function:

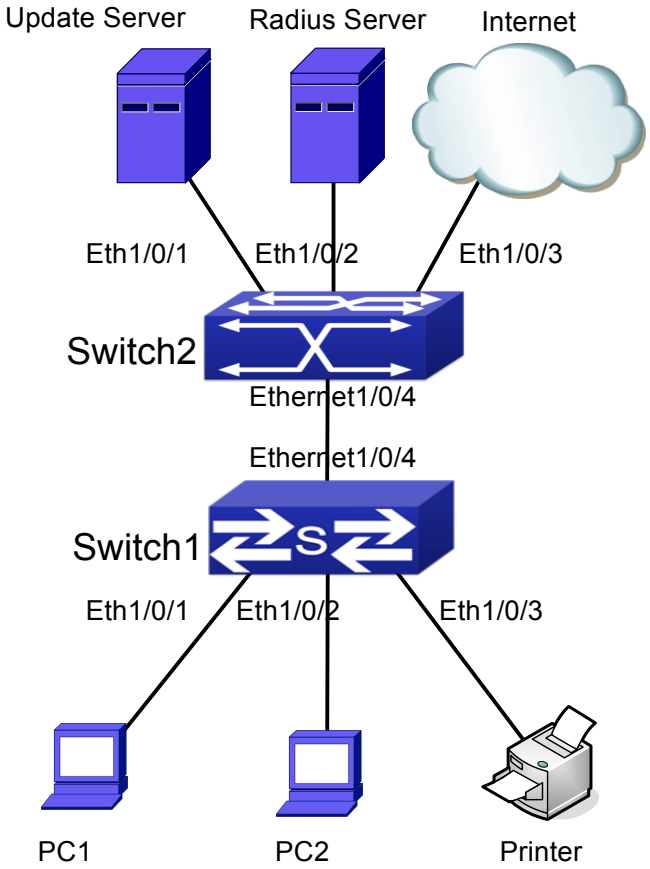


Fig 10-1 MAB application

Switch1 is a layer 2 accessing switch, Switch2 is a layer 3 aggregation switch.

Ethernet 1/0/1 is an access port of Switch1, connects to PC1, it enables 802.1x port-based function and configures guest vlan as vlan8.

Ethernet 1/0/2 is a hybrid port, connects to PC2, native vlan of the port is vlan1, and configures guest vlan as vlan8, it joins in vlan1, vlan8 and vlan10 with untag method and enables MAB function.

Ethernet 1/0/3 is an access port, connects to the printer and enables MAB function.

Ethernet 1/0/4 is a trunk port, connects to Switch2.

Ethernet 1/0/4 is a trunk port of Switch2, connects to Switch1.

Ethernet 1/0/1 is an access port, belongs to vlan8, connects to update server to download and upgrade the client software.

Ethernet 1/0/2 is an access port, belongs to vlan9, connects to radius server which configure auto vlan as vlan10.

Ethernet 1/0/3 is an access port, belongs to vlan10, connects to external internet

resources.

To implement this application, the configuration is as follows:

Switch1 configuration:

(1) Enable 802.1x and MAB authentication function globally, configure username and password of MAB authentication and radius-server address

```
Switch(config)# dot1x enable
Switch(config)# mac-authentication-bypass enable
Switch(config)#mac-authentication-bypass username-format fixed username mabuser password mabpwd
Switch(config)#vlan 8-10
Switch(config)#interface vlan 9
Switch(config-if-vlan9)ip address 192.168.61.9 255.255.255.0
Switch(config-if-vlan9)exit
Switch(config)#radius-server authentication host 192.168.61.10
Switch(config)#radius-server accounting host 192.168.61.10
Switch(config)#radius-server key test
Switch(config)#aaa enable
Switch(config)#aaa-accounting enable
```

(2) Enable the authentication function of each port

```
Switch(config)#interface ethernet  1/0/1
Switch(config-if-ethernet1/0/1)#dot1x enable
Switch(config-if-ethernet1/0/1)#dot1x port-method portbased
Switch(config-if-ethernet1/0/1)#dot1x guest-vlan 8
Switch(config-if-ethernet1/0/1)#exit

Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#switchport mode hybrid
Switch(config-if-ethernet1/0/2)#switchport hybrid native vlan 1
Switch(config-if-ethernet1/0/2)#switchport hybrid allowed vlan 1;8;10 untag
Switch(config-if-ethernet1/0/2)#mac-authentication-bypass enable
Switch(config-if-ethernet1/0/2)#mac-authentication-bypass enable guest-vlan 8
Switch(config-if-ethernet1/0/2)#exit

Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#switchport mode access
Switch(config-if-ethernet1/0/3)#mac-authentication-bypass enable
```

```
Switch(config-if-ethernet1/0/3)#exit

Switch(config)#interface ethernet 1/0/4
Switch(config-if-ethernet1/0/4)# switchport mode trunk
```

10.4 MAB Troubleshooting

If there is any problem happens when using MAB function, please check whether the problem is caused by the following reasons:

- ☞ Make sure global and port MAB function are enabled;
- ☞ Make sure the correct username and password of MAB authentication are used;
- ☞ Make sure the radius-server configuration is correct. Complete MAB offline-detect through query whether dynamic MAC is exist. Do not delete the binding if the MAC address exists in MAC address table. The actual offline time without the traffic is 1-2 MAC aging period add 0-1 MAB offline-detect time.

Chapter 11 PPPoE Intermediate Agent Configuration

11.1 Introduction to PPPoE Intermediate Agent

11.1.1 Brief Introduction to PPPoE

PPPoE (Point to Point Protocol over Ethernet) is a protocol that apply PPP protocol to Ethernet. PPP protocol is a link layer protocol and supply a communication method of point-to-point, it is usually selected by host dial-up link, for example the link is line dial-up. PPP protocol is applied to Ethernet that means PPPoE protocol makes many hosts of Ethernet to connect a remote access collector through one or multiple bridge devices. If the remote access collector is broadband access server (BAS), it can supply broadband access and accounting functions for these hosts, so PPPoE protocol is used to broadband access authentication of Ethernet usually.

11.1.2 Introduction to PPPoE IA

Along with broadband access technique is rapidly developed, broadband access network is also developing from strength to strength, but security problem gradually becomes the focus, soever the clients or the access device and the network are faced with security problem (especially from the client) in the current access network. Traditional Ethernet user can not be identified, traced and located exactly, however in exoteric and controllable network, identification and location are the basic character and requirement for user, for example, when supplying the application that use user accounts to login, this method supplied by PPPoE Intermediate Agent can availably avoid user accounts embezzled.

There are two stages for PPPoE protocol work: discovery stage and session stage. Discovery stage is used to obtain MAC address of the remote server to establish a point-to-point link and a session ID with the server, and session stage uses this session ID to communicate. PPPoE Intermediate Agent only relates to discovery stage, so we simply introduce discovery stage.

There are four steps for discovery stage:

1. Client sends PADI packet: The first step, client uses broadcast address as destination address and broadcast PADI (PPPoE Active Discovery Initiation)

packet to discover access collector in layer 2 network. Notice: This message may be sent to many access collector of the network.

2. Broadband Access Server responds PADO packet: The second step, server responds PADO (PPPoE Active Discovery Offer) packet to client according to the received source MAC address of PADI packet, the packet will take sever name and service name.
3. Client sends PADR packet: The third step, client selects a server to process the session according to the received PADO packet. It may receives many PADO packets for PADI message of the first step may be sent to many servers (select the server according to whether the service information of PADO packet match with the servce information needed by client). MAC address of the other end used for session will be known after server is selected, and send PADR (PPPoE Active Discovery Request) packet to it to announce server the session requirement.
4. Server responds PADS packet: The fourth step, server establishes a session ID according to the received PADR packet, this session ID will be sent to client through PADS (PPPoE Active Discovery Session-confirmation) packet, hereto PPPoE discovery stage is completed, enter session stage.

PADT (PPPoE Active Discovery Terminate) packet is an especial packet of PPPoE, its' Ethernet protocol number (0x8863) is the same as four packets above, so it can be considered a packet of discovery stage. To stop a PPPoE session, PADT may be sent at the discretional time of the session. (It can be sent by client or server)

PPPoE Intermediate Agent supplies a function that identify and locate the user. When passing network access device, PADI and PADR messages sent by client with the access link tag of this device at PPPoE discovery stage, so as to exactly identify and locate the user on server.

If the direct-link access device is LAN switch, the added information include: MAC, Slot ID, Port Index, Vlan ID, and so on. This function is implemented according to Migration to Ethernet-based DSL aggregation.

11.1.2.1 PPPoE Intermediate Agent Exchange Process

PPPoE Intermediate Agent exchange process is similar to PPPoE exchange process, for the first exchange process, the access link tag is added to PADI and PADR packets. The exchange process is as follows:

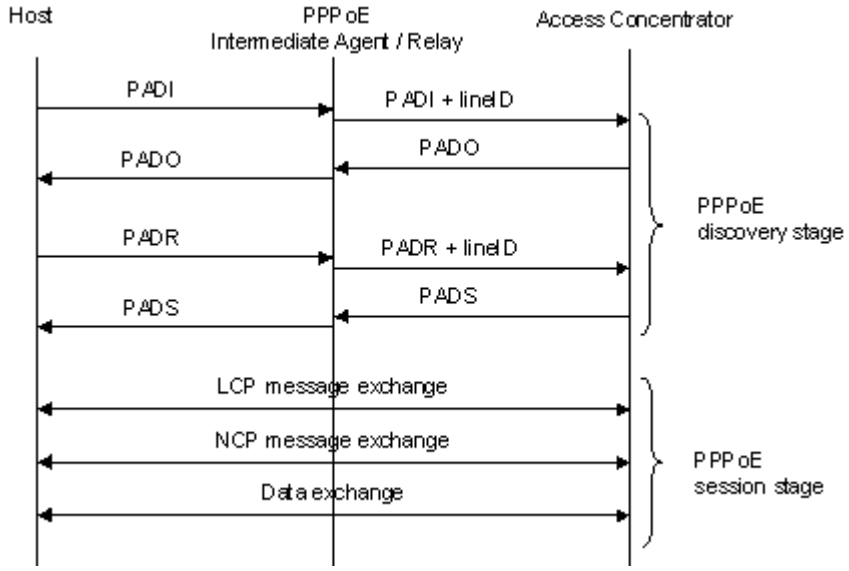


Fig 11-1 PPPoE IA protocol exchange process

11.1.2.2 PPPoE Packet Format

PPPoE packet format is as follows:

Ethernet II frame

Destination MAC	Source MAC	Type Field	PPPoE Data	CRC Check Sum

PPPoE data

Version	Type	Code	Session ID	Length Field	TLV1	……	TLV N

TLV frame

Type	Length	Data

Each field meanings in the following:

Type field (2 bytes) of Ethernet II frame: The protocol sets type field value of PPPoE protocol packet as 0x8863 (include 5 kinds of packets in PPPoE discovery stage only), type field value of session stage as 0x8864.

PPPoE version field (4 bits): Specify the current PPPoE protocol version, the current version must be set as 0x1.

PPPoE type field (4 bits): Specify the protocol type, the current version must be set as 0x1.

PPPoE code field (1 byte): Specify the packet type. 0x09 means PADI packet, 0x07 means PADO packet, 0x19 means PADR packet, 0x65 means PADS packet, 0xa7 means PADT packet.

PPPoE session ID field (2 bytes): Specify the session ID.

PPPoE length field (2 bytes): Specify the sum of all TLV length.

TLV type field (2 bytes): A TLV frame means a TAG, type field means TAG type, the table is as follows.

TLV length field (2 bytes): Specify the length of TAG data field.

TLV data field (the length is not specified): Specify the transmitted data of TAG.

Tag Type	Tag Explanation
0x0000	The end of a series tag in PPPoE data field, it is saved for ensuring the version compatibility and is applied by some packets.
0x0101	Service name. Indicate the supplied services by network.
0x0102	Server name. When user receives the PADO response packet of AC, it can obtain the server name from the tag and select the corresponding server.
0x0103	Exclusive tag of the host. It is similar to tag field of PPPoE data packets and is used to match the sending and reveiving end (Because broadcast network may exist many PPPoE data packets synchronously).
0x0104	AC-Cookies. It is used to avoid the vicious DOS attack.
0x0105	The identifier of vendor.
0x0110	Relay session ID. PPPoE data packet can be interrupted to other AC, this field is used to keep other connection.
0x0201	The error of service name. When the requested service name is not accepted by other end, the response packet will take this tag.
0x0202	The error of server name.
0x0203	Common error.

Table 11-1 TAG value type of PPPoE

11.1.2.3 PPPoE Intermediate Agent vendor tag Frame

The following is the format of tag added by PPPoE IA, adding tag is the Uppermost function of PPPoE IA.

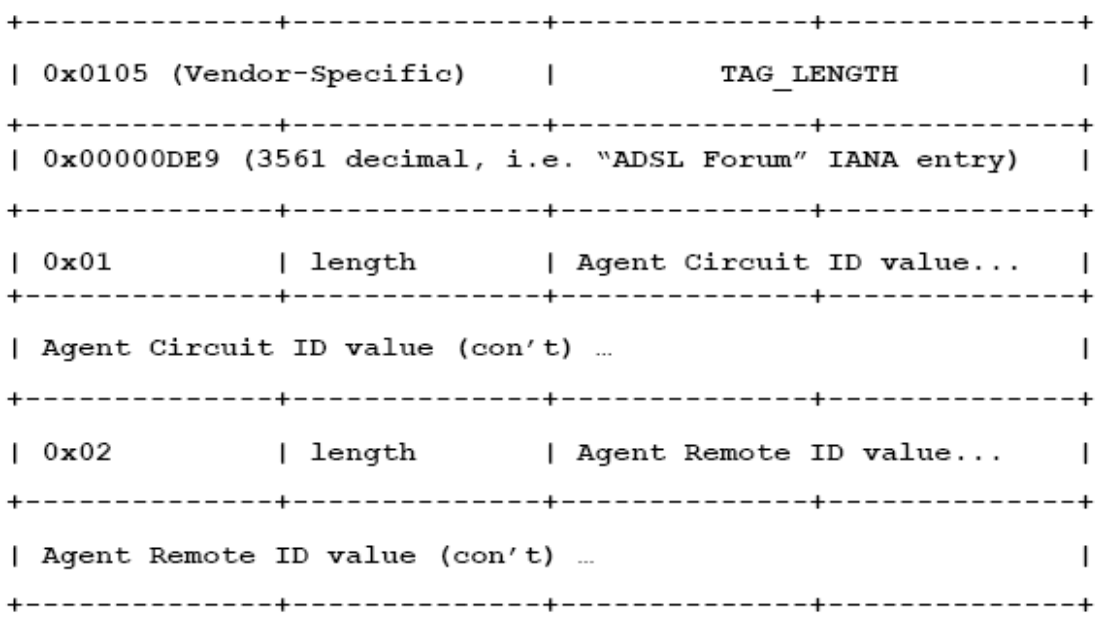


Fig 11-2 PPPoE IA - vendor tag (4 bytes in each row)

Add TLV tag as 0x0105 for PPPoE IA, TAG_LENGTH is length field of vendor tag; 0x00000DE9 is "ADSL Forum" IANA entry of the fixed 4 bytes; 0x01 is type field of Agent Circuit ID, length is length field and Agent Circuit ID value field; 0x02 is type field of Agent Remot ID, length is length field and Agent Remote ID value field.

PPPoE IA supplies a default circuit ID value, the default circuit ID (The figure in the following) includes 5 fields, ANI (Access Node Identifier) can be configured by user, its length is less than 47 bytes. If there is no ANI configured, MAC is accessed by default, occupy 6 bytes and use space symbol to compart, "eth" occupies 3 bytes and uses space symbol to compart, "Slot ID" occupies 2 bytes, use "/" to compart and occupy 1 byte, "Port Index" occupies 3 bytes, use ":" to compart and occupy 1 byte, "Vlan ID" occupies 4 bytes, all fields use ASCII, user can configure ciucuit ID for each port according to requirement.

ANI	Space	eth	Space	Slot ID	/	Port Index	:	Vlan ID
(n byte)	(1byte)	(3 byte)	(1 byte)	(2 byte)	(1byte)	(3 byte)	(1 byte)	(4 byte)

Fig 11-3 Agent Circuit ID value

MAC of the access switch is the default remote ID value of PPPoE IA. remote ID value can be configured by user flexibly, the length is less than 63 bytes.

11.1.2.4 Trust Port of PPPoE Intermediate Agent

Discovery stage sends five kinds of packets, PADI and PADR packets sent by client to server, PADO and PADS packets sent by server to client, PADT packet can be sent by server or client.

In PPPoE IA, for security and reduce traffic, set a port connected server as trust port,

set ports connected client as untrust port, trust port can receive all packets, untrust port can receive only PADI, PADR and PADT packets which are sent to server. To ensure client operation is correct, it must set the port connected server as trust port, each access device has a trust port at least.

PPPoE IA vendor tag can not exist in PPPoE packets sent by server to client, so we can strip and forward these vendor tags if they exist in PPPoE packets. Strip function must be configured on trust port, enabling strip function is not take effect on untrust port.

11.2 PPPoE Intermediate Agent Configuration Task List

1. Enable global PPPoE Intermediate Agent
2. Enable port PPPoE Intermediate Agent

Command	Explanation
Global Mode	
pppoe intermediate-agent **no pppoe intermediate-agent**	Enabel global PPPoE Intermediate Agent function.
pppoe intermediate-agent type tr-101 circuit-id access-node-id <*string*> **no pppoe intermediate-agent type tr-101 circuit-id access-node-id**	Configure access node ID field value of circuit ID in added vendor tag.
pppoe intermediate-agent type tr-101 circuit-id identifier-string <*string*> option {sp | sv | pv | spv} delimiter <*WORD*> [delimiter <*WORD*>] **no pppoe intermediate-agent type tr-101 circuit-id identifier-string option delimiter**	Configure circuit-id in added vendor tag.
pppoe intermediate-agent type self-defined circuit-id {vlan| port|id (switch-id (mac | hostname)| remote-mac) | string WORD} **no pppoe intermediate-agent type self-defined circuit-id**	Configure the self-defined circuit-id.

Security Function Configuration	
pppoe intermediate-agent type self-defined remote-id {mac | hostname| string WORD} **no pppoe intermediate-agent type self-defined remote-id**	Configure the self-defined remote-id.
pppoe intermediate-agent delimiter <*WORD*> **no pppoe intermediate-agent delimiter**	Configure the delimiter among the fields in circuit-id and remote-id
pppoe intermediate-agent format (circuit-id | remote-id) (hex | ascii) **no pppoe intermediate-agent format (circuit-id | remote-id)**	Configure the format with hex or ASCII for circuit-id and remote-id.
Port Mode	
pppoe intermediate-agent **no pppoe intermediate-agent**	Enable PPPoE Intermediate Agent function of port.
pppoe intermediate-agent vendor-tag strip **no pppoe intermediate-agent vendor-tag strip**	Set vendor tag strip function of port.
pppoe intermediate-agent trust **no pppoe intermediate-agent trust**	Set a port as trust port.
pppoe intermediate-agent circuit-id <*string*> **no pppoe intermediate-agent circuit-id**	Set circuit-id of port.
pppoe intermediate-agent remote-id <*string*> **no pppoe intermediate-agent remote-id**	Set remote-id of port.

11.3 PPPoE Intermediate Agent Typical Application

PPPoE Intermediate Agent typical application is as follows:

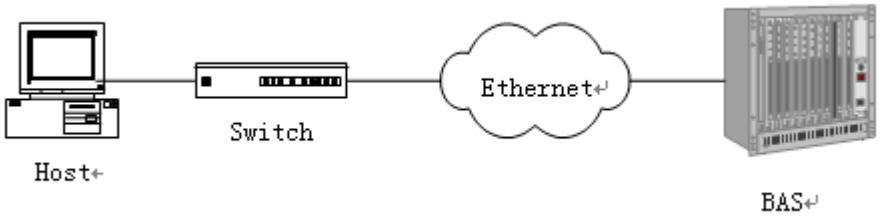


Fig 11-4 PPPoE IA typical application

Both host and BAS server run PPPoE protocol, they are connected by layer 2 ethernet, switch enables PPPoE Intermediate Agent function.

Typical configuration (1) in the following:

Step1: Switch enables global PPPoE IA function, MAC as 0a0b0c0d0e0f.

Switch(config)# pppoe intermediate-agent

Step2: Configure port ethernet1/0/1 which connect server as trust port, and configure vendor tag strip function.

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip

Step3: Port ethernet1/0/2 of vlan1 and port ethernet1/0/3 of vlan 1234 enable PPPoE IA function of port.

Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent

Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent

Step4: Configure pppoe intermediate-agent access-node-id as abcd.

Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd

Step5: Configure circuit ID as aaaa, remote ID as xyz for port ethernet1/0/3.

Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent circuit-id aaaa

Switch (config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz

circuit-id value is ”abcd eth 01/002:0001”, remote-id value is ”0a0b0c0d0e0f” for the added vendor tag of port ethernet1/0/2.

circuit-id value is ”aaaa”, remote-id value is ”xyz” for the added vendor tag of port ethernet1/0/3.

Typical configuration (2) in the following:

Step1: Switch enables global PPPoE IA function, MAC as 0a0b0c0d0e0f.

Switch(config)#pppoe intermediate-agent

Step2: Configure port ethernet1/0/1 which connect server as trust port, and configure vendor tag strip function.

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent trust

Switch(config-if-ethernet1/0/1)#pppoe intermediate-agent vendor-tag strip

Step3: Port ethernet1/0/2 of vlan1 and port ethernet1/0/3 of vlan 1234 enable PPPoE IA function of port.

Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent

Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent

Step4: Configure pppoe intermediate-agent access-node-id as abcd.

Switch(config)#pppoe intermediate-agent type tr-101 circuit-id access-node-id abcd

Step5: Configure pppoe intermediate-agent identifier-string as “efgh”, combo mode as spv, delimiter of Slot ID and Port ID as “#”, delimiter of Port ID and Vlan ID as “/”.

Switch(config)#pppoe intermediate-agent type tr-101 circuit-id identifier-string efgh option spv delimiter # delimiter /

Step6: Configure circuit-id value as bbbb on port ethernet1/0/2.

Switch(config-if-ethernet1/0/2)#pppoe intermediate-agent circuit-id bbbb

Step7: Configure remote-id as xyz on ethernet1/0/3.

Switch(config-if-ethernet1/0/3)#pppoe intermediate-agent remote-id xyz

circuit-id value is ”bbbb”, remote-id value is ”0a0b0c0d0e0f” for the added vendor tag of port ethernet1/0/2.

circuit-id value is ”efgh eth 01#003/1234”, remote-id value is ”xyz” for the added vendor tag of port ethernet1/0/3.

11.4 PPPoE Intermediate Agent Troubleshooting

- Only switch enables global PPPoE intermediate agent firstly, this function can be run on port.
- Configure a trust port at least, and this port can connect to server.
- vendor tag strip function must be configured by trust port.
- Circuit-id override priority is: pppoe intermediate-agent circuit-id < pppoe intermediate-agent identifier-string option delimiter < pppoe intermediate-agent access-node-id.

Chapter 12 SAVI Configuration

12.1 Introduction to SAVI

SAVI (Source Address Validation Improvement) is a security authentication method that provides the granularity level of the node source address. It gets the trust node information (such as port, MAC address information), namely, anchor information by monitoring the interaction process of the relative protocol packets (such as ND protocol, DHCPv6 protocol) and using CPS (Control Packet Snooping) mechanism. After that, it binds the anchor information with the node source address and sends the corresponding filter rules, allow the packets which match the filter rules to pass only, so as to reach the aim that check the validity of node source address.

SAVI function includes ND Snooping function, DHCPv6 Snooping function and RA Snooping according to the protocol packet type. ND Snooping function is used to detect ND protocol packet, it sets IPv6 address binding obtained by nodes with the stateless address configuration. DHCPv6 Snooping function is used to detect DHCPv6 protocol packet, it sets IPv6 address binding obtained by nodes with the stateful address configuration. RA Snooping function is used to avoid the lawless node sending the spurious RA packet.

12.2 SAVI Configuration

SAVI configuration task list:

1. Enable or disable SAVI function
2. Enable or disable application scene function for SAVI
3. Configure SAVI binding function
4. Configure the global max-dad-delay for SAVI
5. Configure the global max-dad-prepare-delay for SAVI
6. Configure the global max-slaac-life for SAVI
7. Configure the lifetime period for SAVI bind-protect
8. Enable or disable SAVI prefix check function
9. Configure IPv6 address prefix for a link
10. Configure the filter entry number of IPv6 address
11. Configure the check mode for SAVI conflict binding
12. Enable or disable user authentication
13. Enable or disable DHCPv6 trust of port

14. Enable or disable ND trust of port
15. Configure the binding number

1. Enable or disable SAVI function

Command	Explanation
Global mode	
savi enable **no savi enable**	Enable the global SAVI function, no command disables the function.

2. Enable or disable application scene function for SAVI

Command	Explanation
Global mode	
savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable **no savi ipv6 {dhcp-only | slaac-only | dhcp-slaac} enable**	Enable the application scene function for SAVI, no command disables the function.

3. Configure SAVI binding function

Command	Explanation
Global mode	
savi ipv6 check source binding ip <*ip-address*> mac <mac-address> interface <*if-name*> {type [slaac | dhcp] lifetime <*lifetime*> | type static} **no savi ipv6 check source binding ip <i*p-address*> interface <*if-name*>**	Configure a static or dynamic binding manually, no command deletes the configured binding. This command may be configured in a global function of savi enable, slaac-only enable, dhcp-only enable or dhcp-slaac enable.

4. Configure the global max-dad-delay for SAVI

Command	Explanation
Global mode	
savi max-dad-delay <*max-dad-delay*> **no savi max-dad-delay**	Configure the max lifetime period of SAVI binding at DETECTION state, no command restores the default value.

5. Configure the global max-dad-prepare-delay for SAVI

Command	Explanation
Global mode	
savi max-dad-prepare-delay	Configure the max redetection lifetime

<*max-dad-prepare-delay*> **no savi max-dad-prepare-delay**	period for SAVI binding, no command restores the default value.

6. Configure the global max-slaac-life for SAVI

Command	Explanation
Global mode	
savi max-slaac-life <*max-slaac-life*> **no savi max-slaac-life**	Configure the lifetime period of the dynamic slaac binding at BOUND state, no command restores the default value.

7. Configure the lifetime period for SAVI bind-protect

Command	Explanation
Global mode	
savi timeout bind-protect <*protect-time*> **no savi timeout bind-protect**	Configure the bind-protect lifetime period to a port after its state from up to down, no command restores the default value.

8. Enable or disable SAVI prefix check function

Command	Explanation
Global mode	
ipv6 cps prefix check enable **no ipv6 cps prefix check enable**	Enable the address prefix check for SAVI, no command disables the function.

9. Configure IPv6 address prefix for a link

Command	Explanation
Global mode	
ipv6 cps prefix <*ip-address*> vlan <*vid*> **no ipv6 cps prefix <*ip-address*>**	Configure IPv6 address prefix for a link manually, no command deletes the configured address prefix.

10. Configure the filter entry number of IPv6 address

Command	Explanation
Global mode	
savi ipv6 mac-binding-limit <*limit-num*>	Configure the corresponding dynamic binding number for the same MAC

no savi ipv6 mac-binding-limit	address, no command restores the default value. Note: The binding number only limits the dynamic binding, but does not limit the static binding number.

11. Configure the check mode for SAVI conflict binding

Command	Explanation
Global mode	
savi check binding <*simple* | *probe*> mode **no savi check binding mode**	Configure the check mode for the conflict binding, no command deletes the check mode.

12. Enable or disable user authentication

Command	Explanation
Port mode	
savi ipv6 check source [ip-address mac-address | ip-address | mac-address] **no savi ipv6 check source**	Enable the control authentication function for user, no command disables the function.

13. Enable or disable DHCPv6 trust of port

Command	Explanation
Port mode	
ipv6 dhcp snooping trust **no ipv6 dhcp snooping trust**	Enable DHCPv6 trust port, no command disables the trust function. (port is translated from trust port into untrust port)

14. Enable or disable ND trust of port

Command	Explanation
Port mode	
ipv6 nd snooping trust **no ipv6 nd snooping trust**	Configure a port as slaac trust and RA trust, no command deletes the port's trust function.

15. Configure the binding number

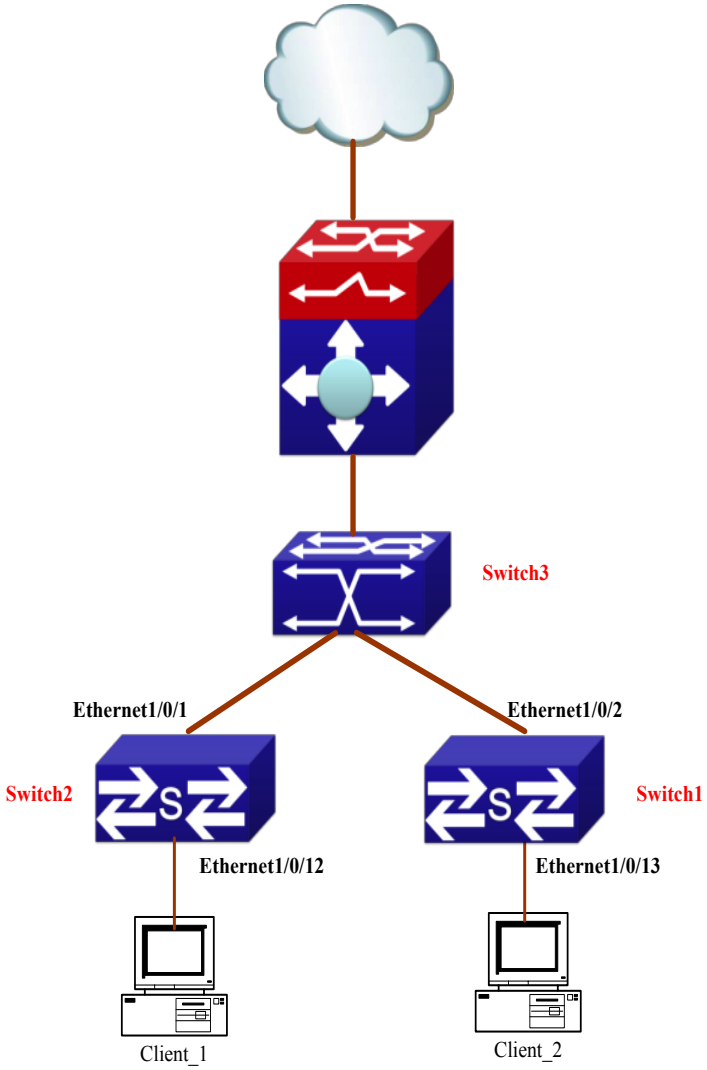
Command	Explanation

Port mode	
savi ipv6 binding num <*limit-num*> **no savi ipv6 binding num**	Configure the binding number of a port, no command restores the default value. Note: The binding number only limits the dynamic binding, but does not limit the static binding number.

12.3 SAVI Typical Application

In actual application, SAVI function is usually applied in access layer switch to check the validity of node source address on direct-link. There are four typical application scenes for SAVI function: DHCP-Only, Slaac-Only, DHCP-Slaac and Static binding. In network environment, users can select the corresponding scene according to the actual requirement; in double stacks network, while SAVI function associates with IPv4 DHCP snooping to use, IPv4 and IPv6 source address authentication is implemented.

Typical network topology application for SAVI function:



Client_1 and Client_2 means two different user's PC installed IPv6 protocol, respectively connect with port Ethernet1/0/12 of Switch1 and port Ethernet1/0/13 of Switch2, and enable the source address check function of SAVI. Ethernet1/0/1 and Ethernet1/0/2 are uplink ports of Switch1 and Switch2 respectively, enable DHCP trust and ND trust functions. Aggregation Switch3 enables DHCPv6 server function and route advertisement function.

Configuration steps of SAVI DHCP-SLAAC scene:

Switch1>enable

Switch1#config

Switch1(config)#savi enable

Switch1(config)#savi ipv6 dhcp-slaac enable

Switch1(config)#savi check binding probe mode

Switch1(config)#interface ethernet1/0/1

Switch1(config-if-ethernet1/0/1)#ipv6 dhcp snooping trust

Switch1(config-if-ethernet1/0/1)#ipv6 nd snooping trust

```
Switch1(config-if-ethernet1/0/1)#exit
Switch1(config)#interface ethernet1/0/12-20
Switch1(config-if-port-range)#savi ipv6 check source ip-address mac-address
Switch1(config-if-port-range)#savi ipv6 binding num 4
Switch1(config-if-port-range)#exit
Switch1(config)#exit
Switch1#write
```

12.4 SAVI Troubleshooting

After ensure no problem about SAVI client hardware and cable, please check the status which may exist and the propositional solutions in the following:

- If IPv6 packets are filtered incorrectly after enable SAVI function, please ensure the global SAVI function enabled. After that, enable the global function of the corresponding SAVI scene according to the actual application scene and enable the port authentication function.
- If client can not correctly obtain IPv6 address assigned by DHCPv6 server after enable SAVI function, please ensure DHCP port trust is configured by uplink port with DHCPv6 server.
- If node binding can not be set for the new user after enable SAVI function, please check whether the direct-link port configures the max binding number, and whether the binding number reaches to the max number. If the binding number exceeds the max binding limit, it is recommended to configure the bigger binding limit.
- If node binding can not be set for new user after configure the bigger binding limit, please check whether the direct-link port configures the corresponding binding number, and whether the corresponding binding number reaches to the max number in the same MAC address. If the binding number exceeds the max binding limit, it is recommended to configure the bigger binding limit.

Chapter 13 Web Portal Configuration

13.1 Introduction to Web Portal Authentication

802.1x authentication uses the special client to authenticate, the device uses the special layer 2 switch, the authentication server uses RADIUS server, the format of authentication message uses EAP protocol. Use EAPOL encapsulation technique (encapsulate EAP packets within Ethernet frame) to process the communication between client and authentication proxy switch, but authentication proxy switch and authentication server use EAPOR encapsulation format (runn EAP packets on Radius protocol) to process the communication. The device and RADIUS server use RADIUS protocol to transmit PAP packets or CHAP packets when the device processes to relay.

For implementing identity authentication and network accessing, user should install the special authentication client software, and spring the authentication flow to communicate with Radius server through logging in authentication client. The after 802.1x authentication adds web based authentication mode, the user can download a special Java Applet program by browser or other plug-in to replace 802.1x client.

For the environment which uses 802.1x authentication, installing client or downloading the special Java Applet program become a mortal problem. To satisfy user's actual requirement, the manual describes an application scene based on web portal authentication. Web portal authentication not only implements the basic device authentication without the client but also implement the security detection to the terminal.

13.2 Web Portal Authentication Configuration Task List

1. Enable/disable web portal authentication globally (required)
2. Enable/disable web portal authentication of the port (required)
3. Configure the max web portal binding number allowed by the port (optional)
4. Configure HTTP redirection address of web portal authentication (required)
5. Configure IP source address for communicating between accessing device and portal server (required)
6. Enable dhcp snooping binding web portal function (optional)
7. Delete the binding information of web portal authentication

1. Enable/disable web portal authentication globally

Command	Explanation
Global Mode	
webportal enable **no webportal enable**	Enable/disable web portal authentication globally.

2. Enable/disable web portal authentication of the port

Command	Explanation
Port Mode	
webportal enable **no webportal enable**	Enable/disable web portal authentication of the port.

3. Configure the max web portal binding number allowed by the port

Command	Explanation
Port Mode	
webportal binding-limit <*1-256*> **no webportal binding-limit**	Configure the max web portal binding number allowed by the port

4. Configure HTTP redirection address of web portal authentication

Command	Explanation
Global Mode	
webportal redirect <*ip*> **no webportal redirect**	Configure HTTP redirection address of web portal authentication.

5. Configure IP source address for communicating between accessing device and portal server

Command	Explanation
Global Mode	
webportal nas-ip <*ip-address*> **no webportal nas-ip**	Configure IP source address for communicating between accessing device and portal server.

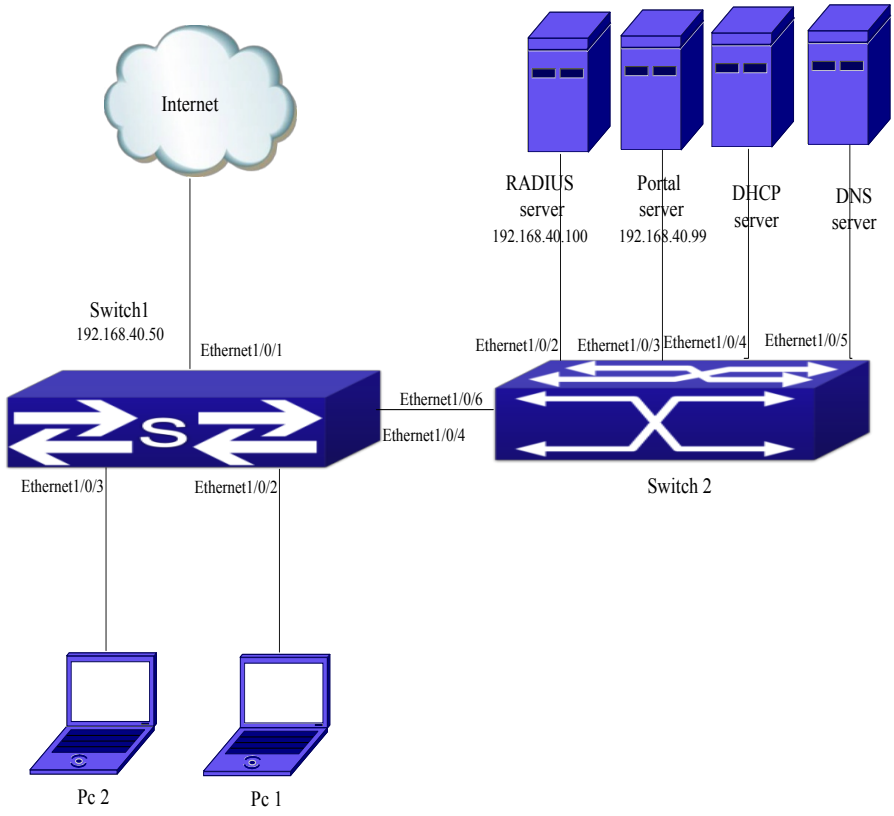
6. Enable dhcp snooping binding web portal function

Command	Explanation
Port Mode	
ip dhcp snooping binding webportal **no ip dhcp snooping binding webportal**	Enable dhcp snooping binding web portal function.

7. Delete the binding information of web portal authentication

Command	Explanation
Admin Mode	
clear webportal binding {mac WORD | interface *<ethernet IFNAME | IFNAME>* |}	Delete the binding information of web portal authentication.

13.3 Web Portal Authentication Typical Example



13-1 Web portal typical application scene

In the above figure, pc1 is end-user, there is http browser in it, but no 802.1x authentication client, pc1 wants to access the network through web portal authentication.

Switch1 is the accessing device, it configures accounting server's address and port as RADIUS server's IP and port, and enable the accounting function. Ethernet 1/0/2 connects to pc1, the port enables web portal authentication, and configure the redirection address and port as portal server's IP and port, so ethernet 1/0/2 forbids all flows except dhcp/dns/arp packets.

Switch2 is the aggregation switch, ethernet1/0/2 connects to radius server, ethernet1/0/3 connects to portal server. The address of radius server is 192.168.40.100, the address of portal server is 192.168.40.99. ethernet1/0/4 connects to DHCP server, ethernet1/0/5 connects to DNS server. ethernet1/0/6 is trunk port and connects to ethernet1/0/4 of switch1.

The configuration of the common web portal authentication is as follows:

```
Switch(config)#interface vlan 1
Switch(config-if-vlan1)#ip address 192.168.40.50 255.255.255.0
Switch(config)#webportal enable
Switch(config)#webportal nas-ip 192.168.40.50
Switch(config)#webportal redirect 192.168.40.99
Switch(config)#interface ethernet 1/0/3
Switch(config-if-ethernet1/0/3)#webportal enable
```

Web portal authentication associates with DHCP snooping binding to use, the configuration is as follows:

```
Switch(config)#ip dhcp snooping enable
Switch(config)#ip dhcp snooping binding enable
Switch(config)#interface ethernet 1/0/2
Switch(config-if-ethernet1/0/2)#webportal enable
Switch(config-if-ethernet1/0/2)#ip dhcp snooping binding webportal
```

13.4 Web Portal Authentication Troubleshooting

When using web portal authentication, the system will show the detailed prompt information if the operation is wrong.

Web portal authentication is disabled by default. After ensure the configuration is correct, use debug command and show command to check the relative information, if you can not determine the cause of the problem, please send the recorded message to technical server center of our company.